2131

PATENT APPLICATION

#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Takahiro SUGIMOTO

Application No.: 09/853,708

Filed: May 14, 2001 Docket No.: 109460

For: METHOD AND APPARATUS FOR ESTABLISHING A SECURITY POLICY, AND METHOD AND APPARATUS FOR SUPPORTING ESTABLISHMENT OF SECURITY POLICY

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2000-164819 filed June 1, 2000; and
Japanese Patent Application No. 2001-132177 filed April 27, 2001.

In support of this claim, certified copies of said original foreign applications:

__X__ are filed herewith.

_____ were filed on _____ in Parent Application No. _____ filed _____.

_____ will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these documents.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/zmc
Date: August 17, 2001

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

#3

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月２７日

出願番号
Application Number: 特願２００１－１３２１７７

出願人
Applicant(s): 株式会社アズジェント

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　５月１８日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０４１８４７

【書類名】　特許願
【整理番号】　ASG-0002
【提出日】　平成13年 4月27日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 5/00
【発明者】
【住所又は居所】　東京都中央区日本橋小網町１９番７号　株式会社アズジェント内
【氏名】　杉本 ▲隆▼洋
【特許出願人】
【識別番号】　500056448
【氏名又は名称】　株式会社アズジェント
【代理人】
【識別番号】　100109014
【弁理士】
【氏名又は名称】　伊藤 充
【電話番号】　03-5366-2677
【先の出願に基づく優先権主張】
【出願番号】　特願2000-164819
【出願日】　平成12年 6月 1日
【手数料の表示】
【予納台帳番号】　067081
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書 1
【物件名】　図面 1
【物件名】　要約書 1
【包括委任状番号】　0008652
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　セキュリティポリシー構築方法及び装置並びにセキュリティポリシー構築を支援する方法及び装置

【特許請求の範囲】

【請求項１】　所定の団体のセキュリティポリシーを構築する方法において、

セキュリティポリシーのドラフトを構築するドラフト構築ステップと、

前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップと、

前記差異に基づき前記セキュリティポリシーのドラフトの調整、又は、前記差異に基づき前記団体の実際の情報システムの運用ルールの調整、を行う調整ステップと、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項２】　請求項１記載のセキュリティポリシー構築方法において、

前記ドラフト構築ステップは、

団体に属するメンバーにするべき質問を生成する生成ステップと、

生成した前記質問を前記メンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する回答取得ステップと、

前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項３】　請求項２記載のセキュリティポリシー構築方法において、

前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項４】　請求項２記載のセキュリティポリシー構築方法において、

前記回答取得ステップは、

前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行

し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、

の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項５】　請求項２記載のセキュリティポリシー構築方法において、

前記分析ステップは、

前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、

前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第１差異検出ステップと、

前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第２差異検出ステップと、

の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項６】　請求項５記載のセキュリティポリシー構築方法において、

前記調査した差異の対策をその優先度と共に立てる対策ステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項７】　請求項１記載のセキュリティポリシー構築方法において、

前記団体のセキュリティ状況を診断する診断ステップ、

を含み、この診断ステップの診断結果を前記団体に提示することによって、前記団体がセキュリティポリシーの必要性を認識しうることを特徴とするセキュリティポリシー構築方法。

【請求項８】　請求項６記載のセキュリティポリシー構築方法において、

前記優先度と共に立てたセキュリティ対策の実行を、その優先度に合わせて計画し、団体の予算化を実現するプライオリティプランニングステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項９】　請求項８記載のセキュリティポリシー構築方法において、
前記セキュリティ対策には、
セキュリティポリシー作成を管理する体制を作ることと、
セキュリティシステムの導入と、
セキュリティポリシーを遵守するための従業員の教育と、
システムログの分析と、
ネットワーク監視と、
セキュリティポリシーに基づく運用の監査と、
セキュリティポリシーの見直しと、
が含まれることを特徴とするセキュリティポリシー構築方法。

【請求項１０】　請求項８記載のセキュリティポリシー構築方法において、
前記計画に合わせて、前記セキュリティ対策を実行するセキュリティ強化策実行ステップ、
を含むことを特徴とするセキュリティポリシー構築方法。

【請求項１１】　セキュリティポリシーを構築する方法において、
団体に属するメンバーにするべき質問を生成する生成ステップと、
生成した前記質問を前記メンバーに聞く質問ステップと、
前記質問に対する前記メンバーの回答を取得する回答取得ステップと、
前記取得した回答に基づき、セキュリティポリシーを構築する構築ステップと、
を含むことを特徴とするセキュリティポリシー構築方法。

【請求項１２】　請求項１１記載のセキュリティポリシー構築方法において、
前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項１３】　請求項１１記載のセキュリティポリシー構築方法において、
前記回答取得ステップは、
前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問

者の回答として前記記憶手段中に保管するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、

の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１４】　請求項１１記載のセキュリティポリシー構築方法において、

前記構築ステップは、

グローバルガイドラインに準拠して、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、

前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、

前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、

の３レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項１５】　請求項１４記載のセキュリティポリシー構築方法において、

前記コーポレートレベルポリシーは、

前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築方法。

【請求項１６】　請求項１４記載のセキュリティポリシー構築方法において、

前記プロダクトレベルポリシーは、

自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述する

第１レベルと、

特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第２レベルと、

の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１７】　請求項１１記載のセキュリティポリシー構築方法において、

前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップ、

を含み、

前記分析ステップは、

前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、

前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第１差異検出ステップと、

前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第２差異検出ステップと、

の少なくとも１個のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１８】　請求項１７記載のセキュリティポリシー構築方法において、

前記調査した差異の対策をその優先度と共に立てる対策ステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項１９】　セキュリティポリシーを構築するセキュリティポリシー構築装置において、

団体に属するメンバーにするべき質問を生成する質問生成手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手

段と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、

を含むことを特徴とするセキュリティポリシー構築装置。

【請求項２０】　請求項１９記載のセキュリティポリシー構築装置において、

前記質問生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項２１】　請求項１９記載のセキュリティポリシー構築装置において、

前記回答保管手段は、

前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

又は、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納し、

又は、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示す、

ことを特徴とするセキュリティポリシー構築装置。

【請求項２２】　請求項１９記載のセキュリティポリシー構築装置において、

前記構築手段は、

前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、

前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、

前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシ

ーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、

の３レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項２３】　請求項２２記載のセキュリティポリシー構築装置において、

前記コーポレートレベルポリシーは、

前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築装置。

【請求項２４】　請求項２２記載のセキュリティポリシー構築装置において、

前記プロダクトレベルポリシーは、

自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第１レベルと、

特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第２レベルと、

の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置。

【請求項２５】　団体のセキュリティ状況を評価する評価方法において、

前記団体に属するメンバーにするべき質問を生成する質問生成ステップと、

前記生成した質問を前記メンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する回答取得ステップと、

前記取得した回答に基づき、セキュリティ状況を評価するセキュリティ状況評価ステップと、

を含むことを特徴とする評価方法。

【請求項２６】　請求項２５記載の評価方法において、

前記質問生成ステップは、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とする評価方法。

【請求項２７】　請求項２５記載の評価方法において、

前記回答保管ステップは、

前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として記憶手段中に保管することを特徴とする評価方法。

【請求項２８】　請求項２５記載の評価方法において、

前記セキュリティ状況の評価は、

前記団体のセキュリティの評価と、

前記団体が属する産業分野に含まれる他の団体のセキュリティの評価の平均と、

前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの評価の最高値と、

を含むことを特徴とする評価方法。

【請求項２９】　請求項２５記載の評価方法において、

前記セキュリティ状況の評価は、

セキュリティに対する理解と姿勢、

前記団体のセキュリティ体制、

不測事態対応、

セキュリティに関する予算化、

セキュリティ改善措置、

の各項目に関する点数を含むことを特徴とする評価方法。

【請求項３０】　団体のセキュリティの状況を評価する評価装置において、

団体に属するメンバーにするべき質問を出力する出力手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、

前記保管した回答に基づき、団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手段と、

を含むことを特徴とする評価装置。

【請求項３１】　請求項３０記載の評価装置において、

前記回答保管手段は、

前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として前記記憶手段中に保管することを特徴とする評価装置。

【請求項３２】　請求項３０記載の評価装置において、

前記セキュリティ完成度報告書は、

前記団体のセキュリティの完成度と、

前記団体が属する産業分野に含まれる他の団体のセキュリティの完成度の平均と、

前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの完成度の最高値と、

を含むことを特徴とする評価装置。

【請求項３３】　請求項３０記載の評価装置において、

前記セキュリティ完成度報告書は、

セキュリティに対する理解と姿勢、

団体のセキュリティ体制、

不測事態対応、

セキュリティに関する予算化、

セキュリティ改善措置、

の各項目に関する点数を含むことを特徴とする評価装置。

【請求項３４】　セキュリティポリシーと、団体の情報システムとの差異を分析する分析装置において、

団体のメンバーに質問をすることによって得られた回答群に含まれる個々の回答の間に矛盾があるか否か検査する矛盾検査手段と、

前記検査した矛盾に関する情報を出力する矛盾出力手段と、

を含むことを特徴とする分析装置。

【請求項３５】　請求項３４記載の分析装置において、

前記矛盾に関する情報に基づき、前記回答群中の矛盾点を指摘する指摘手段と

前記指摘手段が指摘した矛盾点が解決された回答群に基づき、団体の情報システムの構成を仮想的に構築する構築手段と、

前記仮想的に構築した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、

を含むことを特徴とする分析装置。

【請求項３６】　請求項３５記載の分析装置において、

前記団体の情報システムを調査し、前記情報システムの構成を入力する実システム入力手段と、

前記情報システムの構成によって、前記仮想的に構成した情報システムをプルーフし、プルーフ後の前記仮想的に構成した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、

を含むことを特徴とする分析装置。

【請求項３７】　請求項２記載のセキュリティポリシー構築方法において、

前記生成ステップは、前記団体の業種に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項３８】　請求項１１記載のセキュリティポリシー構築方法において、

前記生成ステップは、前記団体の業種に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項３９】　請求項１９記載のセキュリティポリシー構築装置において、

前記質問生成手段は、前記団体の業種に基づき、被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項４０】　請求項２記載のセキュリティポリシー構築方法において、

前記構築ステップは、

特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項４１】　請求項１１記載のセキュリティポリシー構築方法において、

前記構築ステップは、

特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項４２】　請求項１９記載のセキュリティポリシー構築装置において、

前記構築手段は、特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項４３】　請求項２記載のセキュリティポリシー構築方法において、

前記構築ステップは、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項４４】　請求項４３記載のセキュリティポリシー構築方法において、

前記生成ステップは、利用者が指示した１種類又は複数種類のグローバルガイドラインに基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項４５】　請求項１１記載のセキュリティポリシー構築方法において、

前記構築ステップは、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項４６】　請求項４５記載のセキュリティポリシー構築方法において、

前記生成ステップは、利用者が指示した１種類又は複数種類のグローバルガイドラインに基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項４７】　請求項１９記載のセキュリティポリシー構築装置において、

、

前記構築手段は、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項４８】　請求項４７記載のセキュリティポリシー構築装置において

、

前記質問生成手段は、利用者が指示した１種類又は複数種類のグローバルガイドラインに基づき、被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項４９】　請求項２記載のセキュリティポリシー構築方法において、

前記構築ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項５０】　請求項４９記載のセキュリティポリシー構築方法において

、

前記生成ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項５１】　請求項１１記載のセキュリティポリシー構築方法において

、

前記構築ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項５２】　請求項５１記載のセキュリティポリシー構築方法において

、

前記生成ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項５３】　請求項１９記載のセキュリティポリシー構築装置において

、

前記構築手段は、利用者が指示したセキュリティポリシーの強度指標に基づき

、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項５４】　請求項５０記載のセキュリティポリシー構築装置において、

前記質問生成手段は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項５５】　セキュリティポリシーの強度を調整するセキュリティポリシー強度調整方法において、

前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整ステップと、

前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力ステップと、

を含むことを特徴とするセキュリティポリシー強度調整方法。

【請求項５６】　セキュリティポリシーの強度を調整するセキュリティポリシー強度調整装置において、

前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手段と、

前記強度指標に合致していたルールと、前記強度調整手段が置き換えたルールとを、合成して出力する合成出力手段と、

を含むことを特徴とするセキュリティポリシー強度調整装置。

【請求項５７】　所定の団体のセキュリティポリシーを構築する方法において、

前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する生成ステップと、

生成した前記質問をメンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する取得ステップと、

前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築

ステップと、

を含み、

前記構築ステップは、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項５８】　請求項５７記載のセキュリティポリシー構築方法において、

前記生成ステップは、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項５９】　所定の団体のセキュリティポリシーを構築するセキュリティポリシー構築装置において、

前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、

を含み、

前記構築手段は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項６０】　請求項５９記載のセキュリティポリシー構築装置において、

前記質問生成手段は、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項６１】　所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手順と、

前記生成した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６２】　請求項６１記載の記録媒体において、

前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項６３】　請求項６１記載の記録媒体において、

前記回答保管手順は、

前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

又は、

前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、最終的な回答を推定し、推定した回答を示すことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項６４】　請求項６１記載の記録媒体において、

前記質問生成手順は、前記団体の業種に基づき、前記被質問者にするべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項６５】　請求項６１記載の記録媒体において、

前記構築手順は、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項６６】　請求項６１記載の記録媒体において、

前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項６７】　請求項６１記載の記録媒体において、

前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項６８】　所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、

前記出力した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、

前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６９】　請求項６８記載の記録媒体において、

前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項７０】　所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、

前記検査した矛盾に関する情報を出力する矛盾出力手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７１】　請求項７０記載の記録媒体において、

前記矛盾に関する情報に基づき、前記回答群中の矛盾点を指摘する矛盾点指摘手順と、

前記指摘された矛盾点を解決した回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、

前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを比較し、両者の差異を出力する差異出力手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７２】　セキュリティポリシー中の個々のルールであって、利用者

が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、

前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７３】　所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手順と、

前記生成した質問に対する回答を入力し、記憶手段に保管する回答保管手順と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、

をコンピュータに実行させるためのプログラム。

【請求項７４】　請求項７３記載のプログラムにおいて、

前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするプログラム。

【請求項７５】　請求項７３記載のプログラムにおいて、

前記回答保管手順は、

前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

又は、

前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すことを特徴とするプログラム。

【請求項７６】　請求項７３記載のプログラムにおいて、

前記質問生成手順は、前記団体の業種に基づき、前記被質問者にするべき質問を生成することを特徴とするプログラム。

【請求項７７】　請求項７３記載のプログラムにおいて、

前記構築手順は、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするプログラム。

【請求項７８】　請求項７３記載のプログラムにおいて、

前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするプログラム。

【請求項７９】　請求項７３記載のプログラムにおいて、

前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするプログラム。

【請求項８０】　所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、

前記出力した質問に対する回答を入力し、記憶手段に保管する回答保管手順と、

前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、

をコンピュータに実行させるためのプログラム。

【請求項８１】　所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、

前記検査した矛盾に関する情報を出力する矛盾出力手順と、

をコンピュータに実行させるためのプログラム。

【請求項８２】　請求項８１記載のプログラムにおいて、

前記矛盾に関する情報に基づき、前記回答群の整合をとり、矛盾点を解決した回答群を生成する整合手順と、

前記整合した後の回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、

前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを

比較し、両者の差異を出力する差異出力手順と、

をコンピュータに実行させるためのプログラム。

【請求項８３】　セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、

前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、

をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、いわゆるセキュリティポリシーの構築に関する。特に、各団体に適合したセキュリティポリシーを迅速に構築可能な方法・装置、及びセキュリティポリシーの構築を支援する方法・装置に関する。

【０００２】

【従来の技術】

情報技術の発達と共に、情報セキュリティの重要性が増している。団体においては、団体内部の情報を保護するために種々の手段が講じられている。

【０００３】

たとえば、外部のネットワークと接続する部分にはいわゆるファイアーウォールを設け、他者が無断で内部のネットワークに侵入したり、内部の情報にアクセスしてしまうことを防止している。

【０００４】

また、コンピュータウィルス等を駆逐するために、ウィルス検出・駆除ソフトウェアに団体内部のコンピュータを監視させている。なお、本文においては、「団体」とは、企業の他、国や地方公共団体の機関、財団法人等各種法人、その他の団体・組織を意味する。

【０００５】

さて、上述したように、従来から種々の手段が情報セキュリティの確保のため

に用いられている。

【０００６】

しかしながら、各手段を別個独立に議論・検討していたのでは、団体全体としてのセキュリティ強度を確保することは困難である。

【０００７】

たとえば、いくらファイアーウォールを強化しても、団体の建物内に自由に第三者が入ってくることができ、そこにある端末を操作できるのであれば、団体全体としてのセキュリティ強度は著しく低下してしまう。

【０００８】

さらに、ウィルス検出ソフトウェアを用いていても、新たなウィルスに対抗可能とするためにソフトウェアの更新を怠っていれば、新しいコンピュータウィルスには対抗できない。

【０００９】

したがって、団体全体としても情報セキュリティの強度を高くするためには、団体全体としての、情報セキュリティに対する設計及び実現手法を作りあげることが必要である。この設計及び実現手法（群）を一般にセキュリティポリシーと呼ぶ。

【００１０】

【発明が解決しようとする課題】

このセキュリティポリシーは、もちろん各団体毎に異なる項目、内容を有するものであるが、標準的なセキュリティポリシーを構築するための基本的な項目、内容が、国際的なガイドラインとして種々提案されている。

【００１１】

このような汎用的なガイドラインは存在するが、現実に有用なセキュリティポリシーは、個々の団体毎に構築する必要がある。したがって、大量生産できるものではないため、セキュリティポリシーの構築には多大な労力と時間が必要であった。

【００１２】

さらに、セキュリティポリシーは、時間経過と共にその内容を変更する必要が

ある。たとえば、社内の組織が変更された場合には、それに応じて既存情報の利用価値やリスク評価の変更が生じ、それに見合ったセキュリティポリシーを変更しなければならない。

【００１３】

従来は、セキュリティポリシーの構築・定期的な修正等に関する一般的な手法は知られておらず、個々のシステムエンジニアが経験と勘に頼って、セキュリティポリシーの構築・修正を行っている。その結果、セキュリティポリシーの構築・修正に多大な労力が必要となってしまい、ともすれば、修正が団体と実状の変化に追いつけない事態も想定される。

【００１４】

したがって、セキュリティポリシーと団体の実状がかけ離れてしまい、強固な情報セキュリティを構築・維持することが困難な場合も見受けられた。

【００１５】

本発明は、係る課題に鑑みなされたものであり、その目的は、セキュリティポリシーを効率的に構築する方法及びセキュリティポリシーの構築を支援する装置を提供することである。

【００１６】

【課題を解決するための手段】

本発明は、上記課題を解決するために、所定の団体のセキュリティポリシーを構築する方法において、セキュリティポリシーのドラフトを構築するドラフト構築ステップと、前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップと、前記差異に基づき前記セキュリティポリシーのドラフトの調整、又は、前記差異に基づき前記団体の実際の情報システムの運用ルールの調整、を行う調整ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【００１７】

このような構成によって、セキュリティポリシーの構築を段階的に行うことができ、効率的なセキュリティポリシーの構築を行うことができる。

【００１８】

また、本発明は、前記ドラフト構築ステップは、団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【００１９】

このような構成によって、質問に基づきセキュリティポリシーのドラフトを構築できる。

【００２０】

また、本発明は、前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【００２１】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００２２】

また、本発明は、前記回答取得ステップは、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【００２３】

このような構成によって、複数人で分散して質問をした場合に、得られた回答を統合することが可能である。

【００２４】

また、本発明は、前記分析ステップは、前記取得した回答群中に矛盾する回答

が含まれているか否かを検査する矛盾検査ステップと、前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第１差異検出ステップと、前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第２差異検出ステップと、の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【００２５】

このような構成によって、回答間の矛盾を知ることができ、さらに、実システムとセキュリティポリシーの差異を検出することが可能である。

【００２６】

また、本発明は、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００２７】

このような構成によって、優先度を含めた対策を講じることが可能である。

【００２８】

また、本発明は、前記団体のセキュリティ状況を診断する診断ステップ、を含み、この診断ステップの診断結果を前記団体に提示することによって、前記団体がセキュリティポリシーの必要性を認識しうることを特徴とするセキュリティポリシー構築方法である。

【００２９】

このような構成によって、団体のセキュリティ状況を知ることができる。

【００３０】

また、本発明は、前記優先度と共に立てたセキュリティ対策の実行を、その優先度に合わせて計画し、団体の予算化を実現するプライオリティプランニングステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００３１】

このような構成によって、セキュリティ対策を計画的に実行することができ、予算を立てることが容易となる。

【００３２】

また、本発明は、前記セキュリティ対策には、セキュリティポリシー作成を管理する体制を作ることと、セキュリティシステムの導入と、セキュリティポリシーを遵守するための従業員の教育と、システムログの分析と、ネットワーク監視と、セキュリティポリシーに基づく運用の監査と、セキュリティポリシーの見直しと、が含まれることを特徴とするセキュリティポリシー構築方法である。

【００３３】

情報セキュリティ機器の導入だけでなく、従業員の教育等も含まれるので、高い情報セキュリティを達成することができる。

【００３４】

また、本発明は、前記計画に合わせて、前記セキュリティ対策を実行するセキュリティ強化策実行ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００３５】

このような構成によって、セキュリティ対策を円滑に実行に移すことが可能である。

【００３６】

また、本発明は、セキュリティポリシーを構築する方法において、団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティポリシーを構築する構築ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【００３７】

このような構成によって、質問に基づきセキュリティポリシーのドラフトを構築できる。

【００３８】

また、本発明は、前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【００３９】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００４０】

また、本発明は、前記回答取得ステップは、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【００４１】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、その回答のを整合性をとり、インタビュー結果を統合可能である。

【００４２】

また、本発明は、前記構築ステップは、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、の３レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【００４３】

３レベルのセキュリティポリシーが構築されるため、階層的なセキュリティポリシーを得ることができる。ここで、前記コーポレートレベルポリシーの基準に基づき実行するための手段とは、ハードウェア・ソフトウェアだけでなく、それらを利用する際の運用ルール等も含む。

【００４４】

また、本発明は、前記コーポレートレベルポリシーは、前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築方法である。

【００４５】

このような構成によって団体全体のセキュリティポリシーと、個別の機器のセキュリティポリシーとを明確にすることができる。ここで、機器とは、ネットワーク、ホスト、アプリケーション、を含む概念である。

【００４６】

また、本発明は、前記プロダクトレベルポリシーは、自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第１レベルと、特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第２レベルと、の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法である。

【００４７】

このように、自然言語によるプロダクトレベルポリシーによって、人間がセキュリティポリシーを理解することができ、さらに特定言語で記述されたプロダクトレベルポリシーによって各装置の設定が容易になる。ここで、構成装置は、情報セキュリティシステムを構成するハードウェア・ソフトウェアを含むものである。

【００４８】

また、本発明は、前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップ、を含み、前記分析ステップは、前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、前記回答群によって得られた団体の情報システムと、団体の実際の情報システムとの間に差異があるか否かを調査する差異検出ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【００４９】

このような構成によって、矛盾点や、差異を効率的に検出することができる。

【００５０】

また、本発明は、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００５１】

対策がその優先度と共に立てられるため、情報セキュリティの構築計画を立案するのが容易になる。

【００５２】

また、本発明は、団体に属するメンバーにするべき質問を生成する質問生成手段と、前記生成した質問に対する回答を保管する記憶手段と、前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、を含むことを特徴とするセキュリティポリシー構築装置である。

【００５３】

このような構成によれば、メンバーに対する質問が生成されるため、質問作業が容易になる。なお、メンバーとは、その団体の情報システムに関連する個人を意味する。たとえば、従業員だけでなく、パートタイムワーカーや、関連会社の社員等も含まれる。

【００５４】

また、本発明は、前記質問生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【００５５】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００５６】

また、本発明は、前記回答保管手段は、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、又は、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納し、又は、前記

取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すことを特徴とするセキュリティポリシー構築装置である。

【００５７】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、整合性をとり、統合可能である。

【００５８】

また、本発明は、前記構築手段は、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、の３レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【００５９】

３レベルのセキュリティポリシーが構築されるため、階層的なセキュリティポリシーを得ることができる。ここで、前記コーポレートレベルポリシーの基準に基づき実行するための手段とは、ハードウェア・ソフトウェアだけでなく、それらを利用する際の運用ルール等も含む。

【００６０】

また、本発明は、前記コーポレートレベルポリシーは、前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築装置である。

【００６１】

このような構成によって団体全体のセキュリティポリシーと、個別の機器のセキュリティポリシーとを明確にすることができる。ここで、機器とは、ネットワーク、ホスト、アプリケーション、を含む概念である。

【００６２】

また、本発明は、前記プロダクトレベルポリシーは、自然言語で情報セキュリティシステムを構成する各装置の設定を記述する第１レベルと、特定商品の特定言語で情報セキュリティシステムを構成する各装置の設定を記述する第２レベルと、の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置である。

【００６３】

このように、第１レベルのプロダクトレベルポリシーによって、人間がセキュリティポリシーを理解することができ、さらに第２レベルのプロダクトレベルポリシーによって各装置の設定が容易になる。ここで、構成装置は、情報セキュリティシステムを構成するハードウェア・ソフトウェアを含む。

【００６４】

また、本発明は、団体のセキュリティ状況を評価する評価方法において、前記団体に属するメンバーにするべき質問を生成する質問生成ステップと、前記生成した質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティ状況を評価するセキュリティ状況評価ステップと、を含むことを特徴とする評価方法である。

【００６５】

このような構成によって、質問に対する回答に基づき、団体のセキュリティの状況を知ることが可能である。

【００６６】

また、本発明は、前記質問生成ステップは、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とする評価方法である。

【００６７】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００６８】

また、本発明は、前記回答保管ステップは、前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得

した回答とを統合し、単一の被質問者の回答として記憶手段中に保管することを特徴とする評価方法である。

【００６９】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、その回答のを整合性をとり、インタビュー結果を統合可能である。

【００７０】

また、本発明は、前記セキュリティ状況の評価は、前記団体のセキュリティの評価と、前記団体が属する産業分野に含まれる他の団体のセキュリティの評価の平均と、前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの評価の最高値と、を含むことを特徴とする評価方法である。

【００７１】

このような構成によって、その団体を他社と比較して評価することが可能である。また、理論上の最高値が示されるので、経営者が、指標とする目標を定めやすくなる。

【００７２】

また、本発明は、前記セキュリティ状況の評価は、セキュリティに対する理解と姿勢、前記団体のセキュリティ体制、不測事態対応、セキュリティに関する予算化、セキュリティ改善措置、の各項目に関する点数を含むことを特徴とする評価方法である。

【００７３】

このような構成によって、団体の情報セキュリティの評価を、経営者にとっての概念レベルとしてのセキュリティの考え方を、項目別に知ることが可能である。

【００７４】

また、本発明は、団体のセキュリティの状況を評価する評価装置において、団体に属するメンバーにするべき質問を出力する出力手段と、前記出力した質問に対する回答を保管する記憶手段と、前記出力した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記保管した回答に基づき、団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成

度作成手段と、を含むことを特徴とする評価装置である。

【0075】

このような構成によって、生成された質問をメンバーに行い、質問に対する回答に基づき、団体のセキュリティの状況を知ることが可能である。

【0076】

また、本発明は、前記回答保管手段は、前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として前記記憶手段中に保管することを特徴とする評価装置である。

【0077】

このような構成によって、複数人で質問をした場合に、得られた回答を統合することが可能である。

【0078】

また、本発明は、前記セキュリティ完成度報告書は、前記団体のセキュリティの完成度と、前記団体が属する産業分野に含まれる他の団体のセキュリティの完成度の平均と、前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの完成度の最高値と、を含むことを特徴とする評価装置である。

【0079】

このような構成によって、その団体を他社の平均と比較して評価することが可能である。また、理論上の最高値が示されるので、目標を設定することが容易となる。

【0080】

また、本発明は、前記セキュリティ完成度報告書は、セキュリティに対する理解と姿勢、団体のセキュリティ体制、不測事態対応、セキュリティに関する予算化、セキュリティ改善措置、の各項目に関する点数を含むことを特徴とする評価装置である。

【0081】

このような構成によって、団体の情報セキュリティの評価を、経営者にとって

の概念レベルとしてのセキュリティの考え方を、項目別に知ることが可能である。

【００８２】

また、本発明は、セキュリティポリシーと、団体の情報システムとの差異を分析する分析装置において、団体のメンバーに質問をすることによって得られた回答群に含まれる個々の回答の間に矛盾があるか否か検査する矛盾検査手段と、前記検査した矛盾に関する情報を出力する矛盾出力手段と、を含むことを特徴とする分析装置である。

【００８３】

このような構成によって、回答群中に含まれる矛盾を知ることが可能である。

【００８４】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群中の矛盾点を指摘する指摘手段と、前記指摘手段が指摘した矛盾点が解決された回答群に基づき、団体の情報システムの構成を仮想的に構築する構築手段と、前記仮想的に構築した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、を含むことを特徴とする分析装置である。

【００８５】

このような構成によって、セキュリティポリシーと団体の実態との差異を知ることができる。

【００８６】

また、本発明は、前記団体の情報システムを調査し、前記情報システムの構成を入力する実システム入力手段と、前記情報システムの構成によって、前記仮想的に構成した情報システムをプルーフし、プルーフ後の前記仮想的に構成した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、を含むことを特徴とする分析装置である。

【００８７】

このような構成によって、実際の調査によってプルーフした情報システムとセキュリティポリシーの比較を行っているので、両者の差異をより正確に分析することができる。

【００８８】

以下、実施の形態２に関する発明である。

【００８９】

本発明は、上記課題を解決するために、前記生成ステップは、前記団体の業種に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【００９０】

また、本発明は、前記質問生成手段は、前記団体の業種に基づき、被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【００９１】

これらの発明によれば、団体の業種を考慮しているため、その業種に対応したセキュリティポリシーを構築することができる。

【００９２】

以下、実施の形態３に関する発明である。

【００９３】

本発明は、前記構築ステップは、特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【００９４】

また、本発明は、前記構築手段は、特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【００９５】

このような構成によれば、特定の業種に関しては汎用的なグローバルガイドラインより詳細な項目についてセキュリティポリシーを構築することが可能である。

【００９６】

以下、実施の形態４に関する発明である。

【００９７】

本発明は、前記構築ステップは、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【００９８】

また、本発明は、前記構築手段は、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【００９９】

これらの発明の構成によれば、用いるセキュリティポリシーを利用者に選択することができる。

【０１００】

また、本発明は、前記生成ステップは、利用者が指示した１種類又は複数種類のグローバルガイドラインに基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【０１０１】

同様に、本発明は、前記質問生成手段は、利用者が指示した１種類又は複数種類のグローバルガイドラインに基づき、被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【０１０２】

このような構成によれば、利用者の指示するグローバルガイドラインに応じた質問がなされるため、効率的な質問をすることができる。

【０１０３】

以下、実施の形態６に関する発明である。

【０１０４】

本発明は、前記構築ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【０１０５】

また、本発明は、前記構築手段は、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【０１０６】

これらの発明の構成によれば、使用者が「強度指標」を用いてセキュリティポリシーの強度を自由に指示することが可能である。

【０１０７】

また、本発明は、前記生成ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【０１０８】

同様に、本発明は、前記質問生成手段は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築装置である。

【０１０９】

このような構成によれば、利用者が指示する強度に応じて質問が作成される。後述するように、強度を強く指示すれば一般に質問の個数が増え、細かい事項に関する質問も生成される。強度を弱く指示すれば一般に質問の個数は減り、その内容も細かな内容ではなくなる。強度に応じた質問が生成されるため、より効率的な質問を行うことができる。

【０１１０】

次に、本発明は、セキュリティポリシーの強度を調整するセキュリティポリシー強度調整方法において、前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないと判断されたルールを、前記強度指標に合致したルールに置き換える強度調整ステップと、前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力ステップと、を含むことを特徴とするセキュリティポリシー強度調整方法である。

【０１１１】

また、本発明は、セキュリティポリシーの強度を調整するセキュリティポリシー強度調整装置において、前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手段と、前記強度指標に合致していたルールと、前記強度調整手段が置き換えたルールとを、合成して出力する合成出力手段と、を含むことを特徴とするセキュリティポリシー強度調整装置である。

【０１１２】

これらの発明の構成によれば、利用者が強度指標で指示した強度になるように、セキュリティポリシーの強度の調整を行うことができる。

【０１１３】

以下、実施の形態６に関する発明である。

【０１１４】

本発明は、所定の団体のセキュリティポリシーを構築する方法において、前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問をメンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する取得ステップと、前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、を含み、前記構築ステップは、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【０１１５】

このような構成によれば、利用者の指示する範囲のセキュリティポリシーが得られる。

【０１１６】

また、本発明は、前記生成ステップは、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築方法である。

【０１１７】

このような構成によれば、利用者が指示する範囲に関する質問のみが生成されるため、範囲とは関係のない質問をしてしまうことがない。

【０１１８】

また、本発明は、所定の団体のセキュリティポリシーを構築するセキュリティポリシー構築装置において、前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手段と、前記生成した質問に対する回答を保管する記憶手段と、前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、を含み、前記構築手段は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【０１１９】

このような構成によれば、利用者の指示する範囲のセキュリティポリシーが得られる。

【０１２０】

また、本発明は、前記質問生成手段は、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築装置である。

【０１２１】

このような構成によれば、利用者が指示する範囲に関する質問のみが生成されるため、範囲とは関係のない質問をしてしまうことがない。

【０１２２】

以下、実施の形態７に関する発明である。

【０１２３】

実施の形態７では、今まで述べた種々の動作をコンピュータに実行させるプログラム及びそのプログラムが記録されている記録媒体（ハードディスク等）が示されている。したがって、これらのプログラム及びプログラムを記録した記録媒体の作用は、今まで述べた発明と同様である。

【０１２４】

まず、本発明は、所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する

質問生成手順と、前記生成した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【０１２５】

また、本発明は、前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体である。

【０１２６】

また、本発明は、前記回答保管手順は、前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、又は、前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、最終的な回答を推定し、推定した回答を示すことを特徴とするコンピュータ読み取り可能な記録媒体である。

【０１２７】

また、本発明は、前記質問生成手順は、前記団体の業種に基づき、前記被質問者にするべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体である。

【０１２８】

また、本発明は、前記構築手順は、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体である。

【０１２９】

また、本発明は、前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするコンピュータ読み

取り可能な記録媒体である。

【０１３０】

また、本発明は、前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体である。

【０１３１】

また、本発明は、所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、前記出力した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【０１３２】

また、本発明は、所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、前記検査した矛盾に関する情報を出力する矛盾出力手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【０１３３】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群の整合をとり、矛盾点を解決した回答群を生成する整合手順と、前記整合した後の回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを比較し、両者の差異を出力する差異出力手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【０１３４】

また、本発明は、セキュリティポリシー中の個々のルールであって、利用者が

指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【０１３５】

以上の発明が、記録媒体に関する発明である。次に、プログラムに関する発明を示す。

【０１３６】

本発明は、所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手順と、前記生成した質問に対する回答を入力し、記憶手段に保管する回答保管手順と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、をコンピュータに実行させるためのプログラムである。

【０１３７】

また、本発明は、前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするプログラムである。

【０１３８】

また、本発明は、前記回答保管手順は、前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、又は、前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、最終的な回答を推定し、推定した回答を示すことを特徴とするプログラムである。

【０１３９】

また、本発明は、前記質問生成手順は、前記団体の業種に基づき、前記被質問者にするべき質問を生成することを特徴とするプログラムである。

【０１４０】

また、本発明は、前記構築手順は、利用者が指示した１種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを

特徴とするプログラムである。

【０１４１】

また、本発明は、前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするプログラムである。

【０１４２】

また、本発明は、前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするプログラムである。

【０１４３】

また、本発明は、所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、前記出力した質問に対する回答を入力し、記憶手段に保管する回答保管手順と、前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、をコンピュータに実行させるためのプログラムである。

【０１４４】

また、本発明は、所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、前記検査した矛盾に関する情報を出力する矛盾出力手順と、をコンピュータに実行させるためのプログラムである。

【０１４５】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群の整合をとり、矛盾点を解決した回答群を生成する整合手順と、前記整合した後の回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを比較し、両者の差異を出力する差異出力手順と、をコンピュータに実行させるためのプログラムである。

【０１４６】

また、本発明は、セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、をコンピュータに実行させるためのプログラムである。

【０１４７】

【発明の実施の形態】

以下、本発明の好適な実施の形態を図面に基づいて説明する。

【０１４８】

実施の形態１

ある団体に対して行うセキュリティポリシーの構築からそのメンテナンスに至る一連の作業を含むビジネスモデルについて説明する。このビジネスモデルはシステムエンジニアが所定のエキスパートシステムを用いて実行することが好ましい。

【０１４９】

本実施の形態１におけるビジネスモデルの原理をまず説明する。図１には、このビジネスモデルの原理を表すフローチャートが示されている。この図に示すように、本ビジネスモデルは、基本的には６個のステップから構成される。

【０１５０】

ステップ１　セキュリティ完成度評価

ステップ２　セキュリティポリシードラフト構築

ステップ３　システム及びその運用の実査・分析

ステップ４　ポリシー調整・ルール調整

ステップ５　プライオリティプランニング

ステップ６　セキュリティ強化策実行

このような６段階のステップからなるセキュリティ構築手法によれば、最初はインタビューベースのセキュリティポリシーのドラフトを構築し、必要に応じ、団体の実態との再調整を行い、段階的にセキュリティポリシーを完成していくので、各団体のスケジュールや予算に合わせてセキュリティポリシーを構築するこ

とが可能である。

【０１５１】

ステップ１は、団体の情報セキュリティの現状を評価するステップである。この評価によって、団体は自社の経営者レベルの指標を得ることによって、情報セキュリティの現状を知ることができる。

【０１５２】

ステップ２は、団体のメンバーに対して質問をすることによって簡易にセキュリティポリシーのドラフトを作成するステップである。単にインタビューによってセキュリティポリシーのドラフトを作成しているので、安価にセキュリティポリシーを作成することができる。

【０１５３】

ステップ３は、仮想システムと、団体の実態との相違を検討するステップである。仮想システムは質問に対する回答にのみ基づき作成されているので、実態との相違が生じる場合があるからである。

【０１５４】

ステップ４は、差異に基づいて、セキュリティポリシーを調整又は導入済みのセキュリティ商品のルールを調整するステップである。

【０１５５】

ステップ５は、今後の情報セキュリティ計画を、各手段や対策を採用する優先度も含めて構築するステップである。

【０１５６】

ステップ６は、この計画に基づいて、必要なセキュリティ保護対策を実施するステップである。

【０１５７】

以上のように段階的にセキュリティポリシーの構築を行っているため、各団体の予算や考え方等の実状に合わせたセキュリティポリシーの構築が可能である。

【０１５８】

たとえば、会社の考え方や、予算によっては、セキュリティポリシーのドラフトで十分な場合もあろう。また、プライオリティプランニングによれば、将来の

計画がわかるため、団体の予算を立てやすくなるというメリットがある。

【０１５９】

特に、本ビジネスモデルについて中心的なステップは、ステップ２～ステップ４である。ステップ２においてドラフトを作成し、ステップ３において実態との差異を分析し、ステップ４においてセキュリティポリシー又は導入済みのセキュリティ商品の調整を行う。少なくともこれらステップ２～ステップ４を含むビジネスモデルであれば、セキュリティポリシーの構築をシステマティックに行うことができ、従来の経験と勘に頼る手法に比べて、生産性及び品質を高めることが可能である。

【０１６０】

また、このような段階的なセキュリティポリシーの構築を実現するために、本実施の形態１では、種々のエキスパートシステムを使用している。

【０１６１】

以下、エキスパートシステムの利用方法も含めて、ステップ１～ステップ６の各ステップを順に説明する。

【０１６２】

Ａ．ステップ１：セキュリティ完成度評価

このステップでは、団体の現在の情報セキュリティに関する客観的な評価を行う。このような評価を行うことによって、セキュリティに関する団体のランク付けを行うことが可能である。なお、具体的には、上記評価は、セキュリティ完成度評価書を作成することによって実行される。

【０１６３】

本実施の形態１では、米国カーネギーメロン大学のSoftware Capability Maturity Modelに基づき、セキュリティ完成度評価を行う。このModelでは、５個の項目に対して定量的評価を行う。すなわち、点数を与えるのである。

【０１６４】

５個の項目は、以下の通りである。

【０１６５】

ａ．情報セキュリティに対する管理者の理解と姿勢

ｂ．団体のセキュリティ状況

ｃ．不測事態対応

ｄ．セキュリティに関する予算化

ｅ．セキュリティ改善措置

ここで、不測事態とは、情報セキュリティを脅かす事象をいう。たとえば、盗聴行為、機器の故障等である。これらの不測事態に対応できる体制にあるか否かを表すのが上記ｃ．不測事態対応である。また、ｄ．予算化とは、情報セキュリティのために予算が十分にとられているか否かを表す。また、ｅ．セキュリティ改善措置とは、セキュリティの改善の予定や計画がどの程度立てられているか、を表す。

【０１６６】

本実施の形態１では、このような５個の項目に関する点数付けを含む完成度評価書を作成することによって、団体の経営者の指標、セキュリティに対する取り組みに関する意識レベルの客観的な評価を知ることができる。

【０１６７】

具体的なセキュリティ完成度評価書の作成手法について説明する。

【０１６８】

本実施の形態１では、団体に属する経営者に質問をし、その回答に基づいて、完成度評価書を作成する。具体的には、図２に示すような評価装置１０を用いて、質問の生成、回答の収集、セキュリティ完成度評価書の作成等を実行している。また、評価書の作成作業の動作を表すフローチャートが図３に示されている。この図３に示されているフローチャートは、図１におけるステップＳ１－１をより詳細に表したフローチャートである。

【０１６９】

まず、図２に示すように、評価装置１０は、被質問者に行うべき質問を出力する質問出力手段１２を備えている。

【０１７０】

記憶手段１４には、あらかじめ多種多様な質問が格納されており、被質問者に必要な質問が質問出力手段１２によって抽出されるのである。

【０１７１】

また、評価装置１０は、回答保管手段１６を備えている。上記のようにして生成した質問を団体に属する経営者に提示して得られた回答は、この回答保管手段１６に供給される。回答保管手段１６は、回答を記憶手段１４に保管する。

【０１７２】

本実施の形態１において特徴的なことは、回答保管手段１６が回答の統合機能を有していることである。この統合機能とは、質問を複数人のシステムエンジニアが行った場合に、その回答を１個のデータベースにまとめて記憶手段１４に保管する機能である。質問をするべき経営者が多数いる場合には、複数人のシステムエンジニアが分担してインタビュー質問を行った方が迅速に質問に対する回答を得ることができる。このように質問を分担して実行した場合に、その結果は複数のコンピュータ上にそれぞれ蓄積される。したがって、これらの結果を統合する必要があるのである。

【０１７３】

もちろん、ある１人の経営者に対する質問や回答が一度にできず、複数回に分けて行われた場合に、それらの結果を統合するためにも利用可能である。

【０１７４】

また、評価装置１０は、セキュリティ完成度報告書の作成を行うセキュリティ完成度作成手段１８を備えている。このセキュリティ完成度作成手段１８は、記憶手段１４に保管されている回答群に基づきその団体の情報セキュリティに関する評価書であるセキュリティ完成度報告書を作成する。

【０１７５】

この評価装置１０はいわゆるエキスパートシステムである。

【０１７６】

特に、上述したように、本実施の形態１では、収集した回答を統合する機能等を備える評価装置１０を採用している。したがって、セキュリティ完成度評価書を効率よくしかも精密に作成することが可能である。

【０１７７】

次に、図３のフローチャートに基づき、セキュリティ完成度評価書の作成動作

について説明する。

【０１７８】

まず、ステップＳ３－１においては、質問出力手段１２が、その経営者に対して行う質問を出力する。

【０１７９】

そして、ステップＳ３－２において、システムエンジニアは得られた質問を経営者に対して行う。

【０１８０】

ステップＳ３－３においては、質問に対する回答を経営者から得て、評価装置１０の回答保管手段１６に供給する。

【０１８１】

さて、ステップＳ３－４においては、セキュリティ完成度作成手段１８が記憶手段１４に格納された回答群に基づいて、上記の５項目に関するスコア（点数）を含むセキュリティ完成度評価書を作成する。

【０１８２】

以上のようにして、評価装置１０を用いて、セキュリティ完成度評価書が作成される。

【０１８３】

業界標準との比較

セキュリティ完成度評価書には、上述したように、５個の項目に関するスコア（点数）が示される。

【０１８４】

特に、本実施の形態１において特徴的なことは、その団体の属する業界における全団体の平均的なスコア及び最高のスコアが併せて表示されることである。ここで、最高のスコアとは、その業界に含まれる団体であれば達成できるであろう最高のスコア（理論値）である。

【０１８５】

これによって、その団体の情報セキュリティに対する取り組みが、その業界の中でどの程度の位置にいるかを容易に知ることが可能である。なお、このような

業界の平均値や最高値は、記憶手段１４にあらかじめ格納してある。さらに、平均値は、セキュリティ完成度評価を実行して、定期的に更新される。

【０１８６】

セキュリティ実装の経緯報告

本実施の形態１では、セキュリティ完成度評価書は、セキュリティポリシーの構築を行う前に団体の経営者の意識を調査する趣旨で作成している。しかし、情報セキュリティの対策を順次実行していく途中段階で適宜このセキュリティ完成度報告書を作成すれば、情報セキュリティ対策の進捗の程度を知ることが可能である。したがって、このセキュリティ完成度報告書の作成ステップは、セキュリティ実装の経緯報告としての性格も有する。

【０１８７】

なお、本実施の形態１の評価装置１０では、質問や回答などがすべて記憶手段１４に格納されているが、それぞれ専用の別個の記憶手段に格納してもかまわない。

【０１８８】

Ｂ．ステップ２：セキュリティポリシードラフト構築

このステップでは、その団体のセキュリティポリシーの簡単なドラフトを構築する。このドラフトは、団体に属するメンバーに質問をし、その回答に基づき構築するセキュリティポリシーである。したがって、団体の実際の情報システムの調査を行っていないため、迅速にセキュリティポリシーの構築を行うことができる。

【０１８９】

標準的なセキュリティポリシーを構築するための基本的な項目、内容が国際的なガイドラインとして種々知られている。これらをグローバルガイドラインと呼ぶ。本実施の形態１では、これらグローバルガイドライン中の原則を、適宜取り出し、組み合わせることによって、セキュリティポリシーのドラフトを構築する。

【０１９０】

本実施の形態１では、セキュリティポリシードラフト構築装置２０を利用して

セキュリティポリシーのドラフトを構築している。このセキュリティポリシードラフト構築装置２０の構成ブロック図が図４に示されている。

【０１９１】

セキュリティポリシードラフト構築装置２０は、図４に示すように、被質問者の職務内容に基づいて、行うべき質問を生成する質問生成手段２２を備えている。このように職務内容に基づいて、質問を変更するのは、上記評価装置１０の質問生成手段１２と同様に、有意義な回答を得るためである。

【０１９２】

また、図２の記憶手段１４と同様に、セキュリティポリシードラフト構築装置２０内の記憶手段２４にも、多種多様な質問があらかじめ格納されている。そして、質問生成手段２２が、メンバーの職務内容に応じて適切な質問を記憶手段２４から抽出するのである。

【０１９３】

また、セキュリティポリシードラフト構築装置２０は、回答保管手段２６を備えている。この回答保管手段２６も、上記回答保管手段１６と同様に回答を記憶手段２４に保管する。また、回答保管手段２６は、回答の統合機能を有している。

【０１９４】

<u>統合機能</u>

統合機能は、以下のような機能を含んでいる。

【０１９５】

（１）複数のエンジニアが、分散してメンバーにインタビューを行い、インタビュー結果である回答を収集し、一つのデータベースにまとめる。たとえば、ある１人のメンバーに複数のエンジニアがインタビューをした場合には、それらの回答は１のデータベースに統合される。また、たとえば、同種類（たとえばネットワーク）に関する一連の質問を、複数のメンバーにした場合、それらの回答を統合して１のデータベースに組み込む。

【０１９６】

（２）インタビューにおいては同一の質問が異なるメンバーになされる場合が

ある。その結果、回答に矛盾が生じる場合も考えられる。この矛盾を解決するためには、２つの手法がある。第１の手法は、再インタビューである。矛盾点に関し、回答者に言い間違い等があった場合には、再インタビュー又は実査（又はそれら双方）を実行することにより矛盾点を解決できると考えられる。第２の手法は、タイプ（職務内容）によるウェイト付け（重み付け）で、回答を定める方法である。

【０１９７】

本実施の形態１においては、利用者はこの第１の手法と第２の手法を自由に選択することができる。

【０１９８】

また、セキュリティポリシードラフト構築装置２０は、セキュリティポリシーのドラフトを構築するドラフト構築手段２８を備えている。このドラフト構築手段２８は、記憶手段２４に保管されている回答群に基づきそのセキュリティポリシーのドラフトを作成する。

【０１９９】

このセキュリティポリシードラフト構築装置２０も、評価装置１０と同様にいわゆるエキスパートシステムであり、実際には上記各手段は、コンピュータ上で動作するソフトウェアによって実現することが好ましい。

【０２００】

次に、図５のフローチャートに基づき、セキュリティポリシーのドラフトを構築する動作を説明する。図５には、セキュリティポリシードラフト構築装置２０を用いてセキュリティポリシーのドラフトを構築する動作を表すフローチャートが示されている。

【０２０１】

まず、ステップＳ５－１においては、被質問者であるメンバーの職務内容を質問生成手段２２に供給し、そのメンバーに対して行う質問を生成する。

【０２０２】

本実施の形態１においては、このようにそのメンバーの職務内容によって生成する質問が決定される。その結果、被質問者に対して行うべき適切な質問を生成

することが可能である。

【０２０３】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される実際の質問は、メンバーの回答内容によって変更される。たとえば、ＶＰＮを使用しているかという質問に対して、使用していないと回答すれば、ＶＰＮの詳細に関する質問はスキップされる。しかし、ＶＰＮを使用していると回答した場合には、その回答をしたメンバーには、ＶＰＮの詳細に関する質問がなされる。

【０２０４】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【０２０５】

ステップＳ５－２において、生成した質問をメンバーに対して行う。

【０２０６】

ステップＳ５－３においては、質問に対する回答をメンバーから得て、セキュリティポリシードラフト構築装置２０の回答保管手段２６に入力する。入力作業は質問者自身が行うのが好ましい。もちろん、質問を受ける各メンバーがポリシードラフト構築装置２０の画面に向かって、表示される質問に答えるような形態を採用してもかまわない。回答保管手段２６は上述のように統合機能を有しており、複数の質問者が取得してきた回答を統合して、記憶手段２４に格納する。

【０２０７】

ステップＳ５－４においては、ドラフト構築手段２８が記憶手段２４に格納された回答群に基づいて、グローバルガイドライン中の原則を種々組み合わせてセキュリティポリシーを構築する。

【０２０８】

以上のようにして、セキュリティポリシードラフト構築装置２０を用いて、セキュリティポリシーのドラフトが作成される。

【０２０９】

なお、本実施の形態１では、エグゼクティブレベルポリシー、コーポレートレ

ベルポリシー、プロダクトレベルポリシーの３レベルのセキュリティポリシー（のドラフト）が構築される。これら３レベルに関する説明は、Ｂ－５章において後述する。

【０２１０】

Ｂ－１：質問（インタビュー）の内容

以下、質問（以下、インタビューとも呼ぶ）の内容について説明する。

【０２１１】

インタビュー大項目は、以下の通りである。

【０２１２】

１．団体

２．ネットワーク

３．サーバとホスト

４．アプリケーションとデータベース

５．重要性の高いセキュリティ項目

６．その他のセキュリティ項目

以下、各項目を説明する。

【０２１３】

（１）団体

項目「団体」では、団体の概要、体制に関するインタビューが実行される。このインタビュー質問の回答から、情報セキュリティの管理体制、ポリシーの原則、脆弱性分析（差異分析）等を導くことが可能である。

【０２１４】

項目「団体」には、さらに小項目として、以下の項目が含まれている。

【０２１５】

１．１　管理体制

１．２　従業員

１．３　会社概要

１．４　ベンダー

１．５　顧客

１．６　コンサルタント

１．７　外部委託

１．８　アプリケーション

１．９　ネットワーク

１．１０　セキュリティプロファイル

１．１１　業種

１．１２　団体ポリシー

ただし、職務内容によって質問項目が異なる。たとえば、最高経営責任者にはホストについての質問項目はない。このように、本実施の形態１において特徴的なことは、職務によって質問内容が異なることである。これによって、その職務内容に応じた質問をすることができ、効率的なインタビューが可能である。

【０２１６】

（２）ネットワーク

項目「ネットワーク」では、ネットワークの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、ネットワークの脆弱性、ネットワークに関するコーポレートレベルポリシー等が導かれる。

【０２１７】

項目「ネットワーク」には、さらに小項目として、以下の項目が含まれている。

【０２１８】

２．１　運用環境

２．２　ネットワークのプロパティ

２．３　認証と識別

２．４　監査とログ

２．５　アクセス制御

２．６　変更手続き

２．７　災害復旧とバックアップ

２．８　オペレーションの信頼性

２．９　物理的セキュリティ

２．１０　モデム

２．１１　ワークステーションセキュリティ

（３）サーバとホスト

項目「サーバとホスト」では、ホストの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、ホストの脆弱性、ホストとサーバに関するコーポレートレベルポリシー等が導かれる。

【０２１９】

項目「サーバとホスト」には、さらに小項目として、以下の項目が含まれている。

【０２２０】

３．１　サーバとホストプロパティ

３．２　認証と識別

３．３　監査とログ

３．４　アクセス制御

３．５　変更手続き

３．６　災害復旧とバックアップ

３．７　オペレーションの信頼性

３．８　物理的セキュリティ

（４）アプリケーションとデータベース

項目「アプリケーションとデータベース」では、アプリケーションの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、アプリケーションの脆弱性、アプリケーションに関するコーポレートレベルポリシー等が導かれる。

【０２２１】

項目「アプリケーションとデータベース」には、さらに小項目として、以下の項目が含まれている。

【０２２２】

４．１　アプリケーション、データベースのプロパティ

４．２　認証と識別

４．３　監査とログ

４．４　アクセス制御

４．５　変更手続き

４．６　災害復旧とバックアップ

４．７　オペレーションの信頼性

４．８　物理的セキュリティ

（５）重要性の高いセキュリティ項目

項目「重要性の高いセキュリティ項目」では、一般的にファイアーウォールやアクセスコントロールを構築する際に必要な情報に関するインタビュー質問が実行される。このインタビュー質問の回答から、コーポレートレベルポリシー、プロダクトレベルポリシー等が導かれる。項目「重要性の高いセキュリティ項目」に含まれる質問群の多くはコーポレートレベルポリシーやプロダクトレベルポリシーに関する質問であるが、エグゼクティブレベルポリシーに影響を与える質問もある。

【０２２３】

項目「重要性の高いセキュリティ項目」には、さらに小項目として、以下の項目が含まれている。

【０２２４】

５．１　ファイアーウォールの管理

５．２　パケットフィルタリング

５．３　ＮＡＴ（ネットワークアドレス変換）

５．４　ＳＭＴＰコンテンツフィルタリング

５．５　ＦＴＰコンテンツフィルタリング

５．６　ＨＴＴＰコンテンツフィルタリング

５．７　ログとアラート

（６）その他のセキュリティ項目

項目「その他のセキュリティ項目」では、一般的にＶＰＮを構築する際に必要な情報に関するインタビュー質問が実行される。このインタビュー質問の回答から、コーポレートレベルポリシー、プロダクトレベルポリシー等が導かれる。

【０２２５】

項目「その他のセキュリティ項目」には、さらに小項目として、以下の項目が含まれている。

【０２２６】

６．１　ＶＰＮのプロパティ

６．２　ＶＰＮの管理

６．３　鍵の配布

６．４　ログと監査

Ｂ－２　インタビューの形式

インタビューの内容は、上記各項目の通りであるが、インタビューは、記述式や、選択式等種々の形式でなされる。

【０２２７】

Ｂ－３　インタビューの対象者

本実施の形態１のセキュリティポリシードラフト構築装置２０は、インタビューの対象となるメンバーによって、質問の内容を変更する。換言すれば、被インタビュー者の職務内容に基づいて、質問の内容を制御しているのである。

【０２２８】

その結果、被インタビュー者に対して行うべき適切な質問を生成することが可能である。

【０２２９】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される質問は、メンバーの回答内容によって変更される。たとえば、ＶＰＮを使用しているかという質問に対して、使用していないと回答すれば、ＶＰＮの詳細に関する質問はスキップされる。しかし、ＶＰＮを使用していると回答した場合には、その回答をしたメンバーには、ＶＰＮの詳細に関する質問がなされる。

【０２３０】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【０２３１】

そのため、実際のインタビューに先立って、被インタビュー者の職務内容をセキュリティポリシー構築装置２０に入力する必要がある。具体的には、以下の項目に関して入力を行う。

【０２３２】

＊名前

＊部署名

＊役職

郵便番号

住所

国名

電話番号

ＥＭＡＩＬアドレス

＊タイプ

これらの項目の中で、＊が頭に付されている項目は必須入力項目である。また、タイプとは、職務内容を表す記号であり、本実施の形態１では、図６に示される記号を用いて職務内容を表している。簡単に言えば、このタイプはいわゆる職務内容を表す。このタイプに基づき、質問すべき内容が決定される。本実施の形態１で取り扱うタイプの一覧表が図６に示されている。

【０２３３】

なお、実際に被質問者に質問される内容は、質問の回答によって変化する。これはいわゆる知識ベース（Knowledge Base）の動作となる。たとえば、パスワードの有効期限は存在するか？という質問に対し、有効期限はなく無制限だと回答したメンバーに対して、有効期限は何日か？という質問は行わない。これに対して、有効期限はあると答えたメンバーに対しては、有効期限は何日か？という質問が出されうる。

【０２３４】

Ｂ－４　管理すべき情報資産

本実施の形態１では、セキュリティを確保する情報資産を５種類に分類してい

る。その５種類は、ネットワーク、ホスト、アプリケーション、ユーザグループ、その他である。本実施の形態１のセキュリティポリシー構築装置に情報資産を入力する場合には、以下の４項目を入力する。ただし、「ホスト」「ネットワーク」に属するアセットの場合は、さらに２項目、「ＩＰアドレス」「サブネットマスク」を入力する。

【０２３５】

アセット（資産）ＩＤ

＊アセットタイプ

＊アセット名

詳細

このうち、アセットタイプには５種類のタイプがある。

【０２３６】

Ａ　アプリケーション

Ｈ　ホスト

Ｎ　ネットワーク

Ｕ　ユーザグループ

Ｗ　その他、ＵＲＬ、ドメイン名、ファイル名

ここで、ユーザグループとは、共通の特徴を有するユーザの論理的な集合をいう。たとえば、会計情報を取り扱い、会計情報を修正、分析、報告するユーザを会計グループと呼ぶ。ユーザグループは１人又は２人以上のユーザから構成される。なお、ユーザとは、その情報資産を使用する人間をいう。

【０２３７】

Ｂ－５　セキュリティポリシードラフトの作成

以上のような質問に対する回答をセキュリティポリシードラフト構築装置２０に入力することによって、セキュリティポリシーの構築が実行される。この装置は、いわゆるエキスパートシステムであり、生成した質問に対する回答を入力することによって、セキュリティポリシーを生成し、出力する装置である。このように質問に対する回答を入力することによって何らかのデータを生成する装置は、従来からエキスパートシステムとしてよく知られているため、その詳細は省略

する。

【０２３８】

本実施の形態１においては、エグゼクティブレベルポリシー、コーポレートレベルポリシー、プロダクトレベルポリシーの３レベルのセキュリティポリシーが生成される。したがって、セキュリティポリシーのドラフトに関しても、これら３レベルのドラフトが作成される。

【０２３９】

（１）エグゼクティブレベルポリシー

エグゼクティブレベルポリシーは、団体のセキュリティに関する「考え方」「方針」を記述したものである。

【０２４０】

エグゼクティブレベルポリシーには、たとえば以下の項目が含まれる。

【０２４１】

アクセス制御

情報資産に対するアクセス権の管理及び制御は、その情報資産の所有者が制御する必要がある。また、制御は、情報資産が保存又は処理される制御システムが有するアクセス制御の仕組みを使用しなければならない。このアクセス制御では、アクセス権の制御に関するその団体の考え方、方針を記述する。

【０２４２】

情報正確性

情報資産の内容を正確にあるがままに維持することは極めて重要な事項である。これは、情報資産は業務上の決定に必要不可欠なものだからである。この情報正確性においては、情報資産の内容の正確性に関する団体の考え方、方針が記述される。

【０２４３】

保証

団体は、情報リソースや、セキュリティ対策の適切な安全性を保証するために適切な措置を採用しなければならない。この保証では、そのような措置に関する団体の方針、考え方を記述する。

【０２４４】

アカウンタビリティ

すべてのシステムはユーザのアクティビティを記録し、分析を可能にしなければならない。各ユーザは、自己の行為に責任を持たなければならない。このアカウンタビリティにおいては、各ユーザの自己の責任に関する団体の考え方、方針を記述する。

【０２４５】

識別・認証

すべてのユーザは、情報資産の機密性に応じて、適切に識別されなければならない。この識別・認証では、このような識別に関する団体の考え方、方針を記述する。

【０２４６】

緊急時対応計画

団体はシステムやネットワークにおける障害に対する適切な対処を保証するために、詳細な計画と手続を作成しなければならない。この緊急時対応計画においては、このような計画と手続に関する団体の考え方、方針を記述する。

【０２４７】

セキュリティ認識

従業員及び経営陣は、団体の情報セキュリティの要件を認識すると同時に自己の責任を自覚しなければならない。このセキュリティ認識においては、このような自己の責任に関する団体の考え方、方針を記述する。

【０２４８】

情報分類

情報セキュリティは、情報資産を保護するためのものである。したがって、保護すべき対象である情報資産は分類され、各分類にしたがって適切に保護されなければならない。情報分類では、この情報資産に関する団体の考え方、方針を記述する。

【０２４９】

職業倫理

ユーザは、定められた行動規範を遵守し、情報資産を取り扱わなければならない。ユーザが方や規則を破り、又は、私的目的のために情報資産を取り扱った場合には、処罰の対象となる。ユーザは処罰の対象となることを認識しなければならない。職業倫理では、ユーザの守るべき行動規範について、団体の考え方、方針を記述する。

【０２５０】

文書管理

セキュリティの仕組みはすべて適切に文書化し、必要に応じて参照されなければならない。文書管理では、この文書化に関する団体の考え方、方針を記述する。

【０２５１】

調査

団体は障害や侵害が発生した場合には、セキュリティポリシーに沿ってその障害や侵害を調査し、その内容をすべて文書化しなければならない。調査では、このような障害や侵害に関する調査や文書化についての団体の考え方、方針を記述する。

【０２５２】

プライバシー

情報資産の使用は関係当事者のプライバシーを保証することを前提としなければならない。プライバシーでは、このプライバシーの保証に関する団体の考え方、方針を記述する。

【０２５３】

リスク管理

情報資産の所有者は、潜在するリスクを評価し、適切な制御、又は防衛策を講じなければならない。リスク管理では、このような評価、制御、防衛策に関する団体の考え方、方針を記述する。

【０２５４】

検証

団体は、すべてのセキュリティの実装を定期的に検証しなければならない。検

証では、このような検証に関する団体の考え方、方針を記述する。

【０２５５】

資産評価

団体は情報資産を分析しなければならない。資産評価では、この分析に関する団体の考え方、方針を記述する。

【０２５６】

セキュリティ管理

団体は、作成したセキュリティポリシーが適切に管理され、変更・修正が必要な場合は、改訂される。セキュリティ管理では、セキュリティポリシーの管理に関する団体の考え方、方針を記述する。

【０２５７】

（２）コーポレートレベルポリシー

コーポレートレベルポリシーは、団体の情報資産に対してエグゼクティブレベルポリシーの記述を適用し、セキュリティの「運用規定」を記述したものである。この適用は、団体の運用ユニット毎に行われる。運用ユニットとは、情報システムを構成する部分をその作用に基づいてグループ分けしたものである。たとえば、ネットワークや、ホスト、アプリケーション等が、それぞれ運用ユニットである。

【０２５８】

エグゼクティブレベルポリシーはいわば「憲法（大原則）」を記述したものであるのに対し、コーポレートレベルポリシーは「法律（大原則に基づく規定）」を記述したものである。

【０２５９】

コーポレートレベルポリシーには、団体全体の情報セキュリティシステムの基準を記述するものと、団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述するものがある。

【０２６０】

団体に存在する運用ユニット全体に関するポリシーでは、たとえば、以下の規定が記述される。

【０２６１】

ネットワーク

このネットワークには、団体ネットワークの全体に対する規定が記述される。

【０２６２】

ホスト

このホストには、団体ホストの全体に対する規定が記述される。

【０２６３】

アプリケーション

このアプリケーションには、団体アプリケーションの全体に対する規定が記述される。

【０２６４】

また、運用ユニットをより細分化した個々のユニットに関する特定のポリシーでは、たとえば、以下のような項目が記述される。

【０２６５】

ソフトウェア管理

このソフトウェア管理には、その団体内で用いられる個々のソフトウェアに関するそのソフトウェアの使用やライセンス管理の規定が記述される。

【０２６６】

ダイヤルアップ

このダイヤルアップには、その団体内で用いられる個々のダイヤルアップやリモートアクセスサーバに関する規定が記述される。

【０２６７】

電子メール

この電子メールには、その団体内で用いられる個々の電子メールの規定が記述される。

【０２６８】

ファイアーウォール管理

このファイルウォールには、その団体内で用いられる個々のファイアーウォールの管理の規定が記述される。

【０２６９】

暗号

この暗号には、その団体内で用いられる個々の暗号化の実装規定が記述される。

【０２７０】

電子商取引

この電子商取引には、その団体内で用いられる個々の電子商取引の規定が記述される。

【０２７１】

ネットワーク

このネットワークには、その団体内で用いられる個々のネットワークの規定が記述される。

【０２７２】

ホスト

このホストには、その団体内で用いられる個々のホストの規定が記述される。

【０２７３】

アプリケーション

このアプリケーションには、その団体内で用いられる個々のアプリケーションの規定が記述される。

【０２７４】

（３）プロダクトレベルポリシー

プロダクトレベルポリシーは、情報資産をどのようなリソース（セキュリティ商品、運用体制）及びその設定を使って保護するか、具体的な「方法」を含む運用手順を記述したものである。上記エグゼクティブレベルポリシーやコーポレートレベルポリシーが、方針や管理面におけるルールを記述しているのに対して、プロダクトレベルポリシーは、ハードウェアやソフトウェアの細部にまでも言及し、エグゼクティブレベルポリシーが提供する「原則」と、コーポレートレベルポリシーが提供する「規定」とに基づいて、具体的にどのように情報資産の保護を実現するかに関する「方法」を提供するものである。したがって、プロダクト

レベルポリシーは、具体的な技術の実装に関する記述を含むものである。

【０２７５】

このプロダクトレベルポリシーは、ソフトウェアやハードウェアに関する記述を含み、さらに、それらを具体的に運用するルールも記述されている。

【０２７６】

実際の業務遂行上の理由で、使用する製品が変更される場合もあるかもしれないし、また、機器の故障で代替機器を使用する場合もあるかもしれない。これらの状況に対する責任や製品の基準は、上記エグゼクティブレベルポリシーやコーポレートレベルポリシーが規定する「原則」や「規定」に委ねられている。換言すれば、これらの状況に対する対策等は上記エグゼクティブレベルポリシーやコーポレートレベルポリシーで十分に規定される必要がある。

【０２７７】

さて、上述したエグゼクティブレベルポリシーは、いわば原則を謳ったものであり、たとえば、「アクセス権は、業務終了と共に抹消されなければならない。」

の如きルールである。

【０２７８】

また、コーポレートレベルポリシーは、具体的な規定を謳ったものであり、たとえば、「アクセス権はＯＳで制御されなければならない。」の如きルールである。

【０２７９】

これに対して、プロダクトレベルポリシーは、具体的な手段を規定するものであり、たとえば、「サーバＡのアクセス制御ルールとして部門Ｂの課長職以上の人間のみしかアクセスできない」や「サーバＡのアクセス権の制御は、管理者Ｘによって管理される。業務上の必要がある者は、管理者Ｘに依頼し、アクセス権を得る。業務終了後は速やかに管理者Ｘに依頼し、アクセス権を抹消する。」の如き記述である。

【０２８０】

さらに、本実施の形態１では、プロダクトレベルポリシーとして、２レベルの

プロダクトレベルポリシーを作成する。

【０２８１】

第１レベルは、エグゼクティブレベルポリシーやコーポレートレベルポリシー等と同様に、自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述したものであり、上で述べた例もこの第１レベルのプロダクトレベルポリシーである。

【０２８２】

第２レベルは、特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述したものであり、たとえば、具体的な装置の設定を記述したスクリプトである。すなわち、各機器（ハードウェアだけでなくソフトウェアも含む）の設定スクリプトそのものを記述したものであり、そのまま、各機器の設定に用いることができるものである。本実施の形態１では、プロダクトレベルポリシーとして各装置の具体的なスクリプトを作成しているため、実際にファイアーウォールやルータなどの装置の設定を行う際の労力が軽減できるという効果がある。

【０２８３】

回答の分析

セキュリティポリシーのドラフトは、質問とその回答により作成されている。このプロセスにおいては、回答にばらつきや矛盾が生じる可能性がある。また、回答が正しいとは限らない。

【０２８４】

そこで、ステップ２のにおいては、さらに以下のことを実行する。

【０２８５】

まず、複数の回答に矛盾があるか否か調査する。さらに、セキュリティポリシーのドラフトと、インタビューの回答から想定される情報システムとの比較を行う。そして、セキュリティポリシーのドラフトと、実際の情報システムの実査を行ってプルーフ（検証）を行った情報システムとの比較を行って、その差異を検出する。

【０２８６】

実際の調査は、エキスパートシステムである分析装置を用いて実行する。この分析装置３０の構成ブロック図が図７に示されている。この図に示すように、分析装置３０は、回答群に互いに矛盾する回答があるか否か検査する矛盾検査手段３２を備えている。この検査結果は、矛盾出力手段４０に供給される。

【０２８７】

矛盾出力手段４０は、検査結果を、インタビュー結果矛盾レポートとして外部に出力する。

【０２８８】

インタビュー結果矛盾レポートの内容は、整合手段４１に供給される。整合手段４１は、回答間に矛盾があった場合の処理を実行する。この処理は２種類あり、利用者がいずれかを選択することが可能である。

【０２８９】

（１）各メンバーの職務内容に基づいて、知識ベースを利用して、最も確からしい回答を示す。利用者はこの最も確からしい回答を採用することもできるし、自分で正しい回答を決定することもできる。

【０２９０】

（２）矛盾点に関し、再インタビューを実施する。又は実際に調査を行って情報システムの実態を知る。再インタビューと実際の調査との双方を実施することも好ましい。

【０２９１】

このようにして整合をとったインタビューの結果（すなわち回答）は、仮想構築手段３４に供給される。

【０２９２】

仮想構築手段３４は、整合がとれた回答群に基づき、その団体の情報システムを仮想的に構築する。さて、このようにして仮想構築手段３４が構築した情報システムの構成や運用は差異出力手段３８に供給される。

【０２９３】

また、分析装置３０は、その団体の実際の情報システムの構成や運用を入力する実システム入力手段３６を備えている。この実システム入力手段３６が入力し

た実システムの構成や運用は、上記差異出力手段３８に供給される。

【０２９４】

上述したように、仮想的な情報システムはインタビューによってのみ構築されている。したがって、実システムとは異なっている可能性がある。そのため、実査によって、この仮想的な情報システムを実際の情報システムでプルーフしたものと、セキュリティポリシーのドラフトとの比較をすれば、一層正確に現在の実システムの修正すべき点を知ることができる。

【０２９５】

このプルーフをするための実査は、精密にすればするほど好ましい。しかし、情報システムのすべてを実査するのは、大きな労力とコストが必要である。さらに、インタビューをした意味が希薄になってしまう。

【０２９６】

そこで、一般には、インタビューの回答を補助できる程度の実査を行い、上記仮想的情報システムのプルーフをし、プルーフをした情報システムとセキュリティポリシーの差異分析を行うのが、効率的である。

【０２９７】

たとえば、インタビューの回答に矛盾がある部分を重点的に実査することも好ましい。さらに、被質問者であるメンバーが忘れてしまった等の理由により回答できない部分を重点的に実査することも好ましい。

【０２９８】

どの程度、実査を行うかは、要求される精度、期限、コストなどによって決定すべきである。このようにして、求めた差異は、分析レポートとして出力される。

【０２９９】

さらに、差異出力手段３８には、セキュリティポリシーのドラフトが供給される。このような構成の下、差異出力手段３８は、以下の２つの比較を実行し、それぞれ差異を検出・出力する。

【０３００】

（１）セキュリティポリシーのドラフトと、インタビュー結果との差異分析。

【０３０１】

（２）セキュリティポリシーのドラフトと、インタビュー結果を実査によってプルーフをとったものとの差異分析。

この（１）の差異分析においては、セキュリティポリシーのドラフトと、仮想構築手段３４が構築した情報システムとの比較が実行される。この両者は、基本的には、メンバーへのインタビューの結果（回答）に基づき、構築されているため、ほとんど差はない場合もある。

【０３０２】

たとえば、インタビューの回答が「パスワードが無制限に有効」となる場合もある。しかし、セキュリティポリシーにおいて、パスワードが無制限に有効とすることはできない。パスワードに期限があることはセキュリティポリシーの基本的な要件であり、これなくしてセキュリティポリシーとは言えない。

【０３０３】

したがって、セキュリティポリシーのドラフトと、上記インタビュー結果の差異は存在しうる。この検出した差異は、分析レポートとして出力される。

【０３０４】

この分析レポートによって、インタビューの結果がセキュリティポリシーの観点から修正すべき点を見つけることができる。

【０３０５】

また（２）の差異分析においては、セキュリティポリシーのドラフトと、上記構築した仮想的な情報システムを実査によってプルーフしたものと、の比較が実行される。

【０３０６】

なお、これら（１）及び（２）の比較は、いずれか一方のみを行ってもよいし、双方を実行してもかまわない。まず、（１）の比較を実行し、不十分であると判断する場合には、さらに（２）を実行することも好ましい。

【０３０７】

また、後述するレベル２の実査と分析で得られた優先度を考慮し、優先度の高い部分を実査の対象とすることも好ましい。

【０３０８】

次に、図５には、本ステップ３の動作を表すフローチャートが示されている。このフローチャートは上記図１のステップＳ１－２をより詳細に表したものである。

【０３０９】

ステップＳ５－５においては、矛盾検査手段３２を用いて、回答群中に矛盾のある回答があるか否か検査する。また、ステップＳ５－６においては、差異出力手段３８を用いて、セキュリティポリシーのドラフトと、インタビュー結果との間に差異があるか否か検査する。ここで、インタビュー結果とは、インタビューの回答によって構築した仮想情報システムと、この仮想情報システムを実査によってプルーフしたシステム、の２種類を含む。

【０３１０】

このように、本実施の形態１によれば、図７に示すような分析装置３０を用いているため、回答群に含まれる回答の間に矛盾があるか否か、回答の内容と実システムとの間に差異があるか否か、を迅速に知ることができる。

【０３１１】

なお、分析装置３０は、いわゆるエキスパートシステムであり、上記各手段は、コンピュータ上で動作するソフトウェアで実現することが望ましい。

【０３１２】

Ｃ．ステップ３：システム及びその運用の実査・分析

このステップでは、構築したセキュリティポリシーのドラフトと、実際の情報システム及びその運用手法との差異を検査し、分析を行う。この分析は、差異を見つけだすことに加え、さらに、その対策案を優先度と共に示すために行う。

【０３１３】

このステップの実査・分析は以下の通りである。

【０３１４】

このステップ３の実査と分析では、上記ステップＳ１－２で得た差異を、人的体制の差異、運用方法の差異、技術的対策の差異、の３種類に分類する。そして

、各差異毎に、その対策と優先度を検討する。

【０３１５】

以下、ネットワークポリシーについて差異がある場合の対策と優先度の例を示す。

【０３１６】

（１）差異１

種類　：人的体制の差異

内容　：ネットワークポリシーでは、ネットワークセグメントの管理者を明らかにする、となっているが、実システムでは明らかではない。

対策　：管理者又は所有者を明確に割り当てる。

【０３１７】

優先度：即刻

（２）差異２

種類　：技術的対策の差異

内容　：ネットワークポリシーでは、ネットワークのユーザ認証で使用するパスワードは長期間使用していなければ抹消されると規定されている。しかし、実システムでは抹消する仕組みがない。

対策　：３０日間使用しないユーザアカウントがあればそのパスワードを抹消する仕組みを設ける。

【０３１８】

優先度：高い

このように、本実施の形態１によれば、回答群と、実システムとの差異を解消するための対策が立てやすくなるため、セキュリティポリシーと実システムとの間の不一致をなくすことが容易となる。

【０３１９】

D　ステップ４：ポリシー調整・ルール調整

さて、上記ステップ３によって、実システムとセキュリティポリシードラフトとの間の不一致点が明確になり、またそれに対する対策と優先度が明らかになった。本ステップ４では、対策の検討と、実際の作業を実行する。

【０３２０】

対策は、大きく２種類に分かれる。

【０３２１】

（１）セキュリティポリシードラフトに調整を加えて実システムに合わせる。

（２）実システム側の運用ルール等を調整する。

【０３２２】

以下、これらを詳細に説明する。

【０３２３】

Ｄ－１　セキュリティポリシードラフトの調整

セキュリティポリシーのドラフトは、既に説明したようにグローバルガイドラインと呼ばれる、標準的なセキュリティポリシーを構築するための基本的な項目、内容を、適宜組み合わせて構築している。現在、有名なグローバルガイドラインは数種類知られており、本実施の形態１では、その数種の中から適宜ルールや方針等を取り出して組み合わせてセキュリティポリシーの構築を行っている。ドラフトの段階では、これら数種のグローバルガイドライン中最も条件の厳しいものを選び出し、セキュリティポリシーのドラフトに組み込んでいる。

【０３２４】

換言すれば、これらグローバルガイドラインは、その種類によって各規定の強度が異なっているのである。たとえば、あるグローバルガイドラインでは、パスワードの有効期限を６０日としているが、他のグローバルガイドラインではこれを１８０日と規定している。

【０３２５】

すなわち、ドラフトの段階では、最も厳しい条件で各ルール等が構築されているのである。したがって、団体側の意向によっては、セキュリティポリシーのドラフト内の各ルールの強度が強すぎると判断される場合もあろう。このような場合には、適宜弱いルールに変更することが好ましい。

【０３２６】

たとえば、同一のパスワードの有効期限を６０日とするルールが厳しい、すな

わち強いルールである場合には、団体側との話し合いによって有効期限を１８０日に変更する、すなわち弱いルールに変更するのである。

【０３２７】

このように、各団体の意向と強度のバランスの判断から、ルールの強度を変更すれば、実システムと合致したセキュリティポリシーを構築することが可能である。

【０３２８】

このようにして、セキュリティポリシーのドラフトの調整が実行される。

【０３２９】

Ｄ－２　ルール調整

上述したレベル２の実査と分析において説明した対策に基づき、実システム側の運用を調整する。このルール調整は、運用方法を変更するものや、さらに、セキュリティシステム（たとえばファイアーウォール）のルール設定の修正等がある。

【０３３０】

Ｅ　ステップ５：プライオリティプランニング

上記ステップ４までで、団体の実際の情報システムに関するセキュリティポリシーの構築が完了する。

【０３３１】

しかし、今後、このセキュリティポリシーに合わせてセキュリティ対策を順次実行していく必要がある。そこで、本ステップ５では、優先順位を含めて各種対策を検討し、リストにしておく。このようなリストを作成しておくことで、今後のセキュリティ対策の計画を立てることができる。さらには、その計画に基づき、予算の検討を行うことができる。すなわち、情報セキュリティ対策の予算化を実現することができるのである。このようなリストがなければ、将来の情報セキュリティ費用がどの程度かかるのか見通しが立たず、予算化が困難になることも考えられる。

【０３３２】

セキュリティ対策には、セキュリティシステムの導入及びテストの他に、セキ

ュリティポリシーを遵守するための従業員の教育、システムログの分析、等の作業も含まれる。

【０３３３】

また、セキュリティポリシーには、ネットワーク監視と、セキュリティポリシーに基づく運用の監査と、セキュリティポリシーの見直しと、が含まれる。

【０３３４】

なお、団体側の情報システムの変更、運用の変更等に合わせて、セキュリティポリシーも変更をする必要がある。そこで、定期的にセキュリティポリシーの見直しを行う必要がある。

【０３３５】

Ｆ　ステップ６：セキュリティ強化策実行

上記ステップ５において作成した優先順位を含めたセキュリティ対策リストに基づき、実際にセキュリティ強化策を実行していく。この実行は上記リスト及びセキュリティポリシーに従ったものであり、円滑に作業を進めることが可能である。

【０３３６】

以上述べたように、本実施の形態１では、セキュリティポリシーの構築からメンテナンスまでを６ステップに分けて実行している。したがって、セキュリティポリシーを段階的に構築、実行していくことが可能であり、団体側の要望に合った作業の進め方を実現可能である。

【０３３７】

実施の形態２（業種の考慮）

上記実施の形態１においては、団体のメンバーの職務内容によって質問が変更される例を説明したが、特に、その団体の業種は考慮していない。

【０３３８】

しかし、たとえば金融業と製造業とでは、構築するセキュリティポリシーも異なるべきである。

【０３３９】

そこで、本実施の形態２では、団体の業種を考慮したセキュリティポリシーを

構築することを提案する。以下、団体の業種を考慮したセキュリティポリシー（のドラフト）を構築するための種々の工夫を説明する。

【０３４０】

上記図４のセキュリティポリシードラフト構築装置２０においては、メンバーの職務内容によって質問が変更される旨説明した。本実施の形態２ではこれに加えて、その団体の業種によって質問を変更する例を説明する。

【０３４１】

図９には、本実施の形態２のセキュリティポリシードラフト構築装置１２０の構成ブロック図が示されている。

【０３４２】

セキュリティポリシードラフト構築装置１２０は、図４に示したセキュリティポリシードラフト構築装置２０とほぼ同様の構成である。

【０３４３】

異なる点の１つは、セキュリティポリシードラフト構築装置１２０が、インタビューを受けるメンバーが属する団体の業種に基づいて質問を生成する質問生成手段１２２を備えていることである。この質問生成手段１２２は、メンバーの職務内容だけでなく、団体の業種に基づいて質問を生成するのである。

【０３４４】

また、記憶手段１２４には、業種によって異なる質問があらかじめ格納されている。質問生成手段１２２は、入力された業種に基づき、その業種に対応する質問群を記憶手段１２４から読み出すのである。

【０３４５】

回答保管手段１２６は、図４における回答保管手段２６とほぼ同様の動作を実行する。

【０３４６】

このような構成によって、各業種に対応した質問を生成し、よりきめの細かいセキュリティポリシーを構築可能である。

【０３４７】

たとえば、金融業の団体に対しては、「預金者リストの管理はどのようにして

いるか？」等の質問を生成すべきであるが、製造業の団体に対してそのような質問を生成する意味はない。逆に、製造業の団体に対して「製造ロット毎の進捗データの管理はどのようにしているか？」等の質問を生成すべきであるが、金融業の団体に対してそのような質問を生成する意味はない。

【０３４８】

したがって、本実施の形態２によれば、団体の業種によって質問を変更し、より詳細な内容についての質問を行うことができ、団体の情報システムの細部（運用・管理も含む）をよりよく知ることが可能である。

【０３４９】

なお、ここで言う質問の変更とは、上述した職務内容と同様に、質問のコースが変更されることを意味する。すなわち、金融業の団体に対しては、金融業向けの質問群を含むコースが適用され、製造業の団体に対しては、製造業向けの質問群を含むコースが適用されるのである。各コースでは、そこに含まれる質問に対する回答の内容によって次の質問が変更されることは実施の形態１と同様である。

【０３５０】

さて、図９のドラフト構築手段１２８は、基本的には図４におけるドラフト構築手段２８と同様のものである。ただし、図９のドラフト構築手段１２８の質問生成手段１２２が生成した、より詳細な内容の質問に対する回答に基づいてセキュリティポリシーのドラフトを構築しているため、既に述べたように、より精密なセキュリティポリシーのドラフトを構築可能である。

【０３５１】

本実施の形態２におけるセキュリティポリシーのドラフトの構築動作は、上記図５におけるフローチャートとほぼ同様である。

【０３５２】

異なる点は、ステップＳ５－１において、その団体の業種が、メンバーの職務内容と同様に質問生成手段１２２に供給される点である。この結果、質問生成手段１２２は、メンバーの職務内容と、団体の業種に基づき適切な質問を生成することが可能である。

【０３５３】

このように、本実施の形態２においては、団体の業種を考慮した質問を生成しているため、インタビューによって団体の情報セキュリティシステムをより詳しく知ることができる。その結果、より精密なセキュリティポリシーの構築を行うことが可能である。

【０３５４】

なお、上記説明では、団体の業種に基づき質問を変更する例を示したが、団体の規模によって変更することも好ましい。

【０３５５】

また、上記説明では、質問の変更の例として質問のコースの変更を示したが、その他種々の変更の方式を採用することができる。たとえば、基本的な質問文の枠組みを定めておき、その文の中の用語を、業種に合わせて変更することも好ましい。具体的には、一般企業に対する質問の文中では「社長」の言葉を用いているが、銀行の場合にはこの「社長」を「頭取」の言葉に置き換える如き変更の方式が考えられる。

【０３５６】

実施の形態３（特定の業種の勧告や規定の考慮）

実施の形態１で述べた例においてはグローバルガイドラインに基づき、セキュリティポリシーを構築している（ステップＳ５－４）。このグローバルガイドラインは、ある特定の目的をもって作成される場合も多いが、概ね汎用的に利用可能なように構成されている。

【０３５７】

この汎用的なグローバルガイドラインに対して、特定の業種の種々の勧告や規定が知られている。これらの勧告や規定は、グローバルガイドラインと異なり、特定の業種向けの勧告や規定であることが明確に謳われているものである。これらの勧告や規定も情報セキュリティに言及している場合が多いため、グローバルガイドラインと同様にセキュリティポリシーの構築の際に利用することが望ましい。

【０３５８】

たとえば、日本の金融情報システムセンター（ＦＩＳＣ：The Center for Financial Industry Information Systems）では、セキュリティ対策のための安全対策基準の策定や、セキュリティポリシーの普及を行っている。そして、このＦＩＳＣは、「金融機関等コンピュータシステムの安全対策基準」等の刊行物を発行している。

【０３５９】

本実施の形態３では、金融業に対してセキュリティポリシーを構築する場合には、グローバルガイドラインだけでなく、この「金融機関等コンピュータシステムの安全対策基準」にも基づいて、セキュリティポリシーを構築することを提案する。この結果、特定の業種においては、その業種に的を絞った勧告や規定に基づきセキュリティポリシーが構築されるため、より緻密なセキュリティポリシーが構築可能である。

【０３６０】

このように、特定の業種向けの勧告や規定をグローバルガイドラインと同様に利用するセキュリティポリシードラフト構築装置の構成が図９に示されている。

【０３６１】

この図に示すように、セキュリティポリシードラフト構築装置２２０の構成は、図８のセキュリティポリシードラフト構築装置１２０とほぼ同様である。異なっている点は、団体の業種に関する情報が、質問生成手段２２２だけでなく、ドラフト構築手段２２８にも供給されている点である。そして、ドラフト構築手段２２８は、団体の業種に基づき、セキュリティポリシーのドラフトの構築に用いるべき特定の勧告や規定を利用者に示し、利用者はこれを選択することが可能である。なお、選択される特定の勧告や規定は、１個には限られず、２個以上とする場合もある。もちろん、利用者は、示される特定の勧告や規定を無視し、一般的なグローバルガイドラインを選ぶことも可能である。

【０３６２】

また、以下の点が本実施の形態３において特徴的な事項である。

【０３６３】

第１に、ドラフト構築手段２２８が、団体の業種に基づき、利用する特定の業

種向けの勧告や規定を選択することが本実施の形態３において新規な事項である。このような動作を行うことによって、たとえば金融業においては、金融業向けの勧告や規定を利用したセキュリティポリシー（のドラフト）を構築することが可能である。

【０３６４】

第２に、記憶手段２２４内に特定の業務向けの勧告や規定に関する情報が、グローバルガイドラインに関する情報と同様に格納されていることである。この情報が格納されていることによって、質問生成手段２２２はその団体の業種向けに制定されている勧告や規定に則した質問を生成することができる。また、この格納されている情報に従って、ドラフト構築手段２２８は、その団体の業種向けに制定されている勧告や規定に基づいたセキュリティポリシーを構築することが可能である。

【０３６５】

また、本実施の形態３におけるセキュリティポリシーの構築動作は、基本的に図５のフローチャートとほぼ同様である。異なる点は以下の通りである。

【０３６６】

第１に、ステップＳ５－１において、その団体の業種が質問生成手段２２２に供給され、その団体の業種向けの勧告や規定が示される。利用者が示された勧告や規定を選択すれば、この勧告や規定に則した質問が生成される点が第１に異なる点である。そのような勧告や規定が存在しない場合には、実施の形態１～実施の形態３と同様にしてグローバルガイドラインに基づいて質問が生成される。

【０３６７】

第２に、ステップＳ５－４において、その団体の業種がドラフト構築手段２２８にも供給され、ドラフト構築手段２２８が、その団体の業種向けの勧告や規定に則してセキュリティポリシーのドラフトを構築する点である。この動作も、利用者がその勧告や規定を選択した場合の動作である。そのような勧告や規定が存在しない場合には、実施の形態１～実施の形態２と同様にしてグローバルガイドラインに基づいてセキュリティポリシーのドラフトが構築される。

【０３６８】

たとえば、グローバルガイドラインによれば、「基幹ネットワークの責任者を立てていますか？」という質問が生成される。しかし、特に金融業の場合には、上記「金融機関等コンピュータシステムの安全対策基準」に基づき、「ＡＴＭ（Automatic Teller Machine：現金自動預入支払機）ネットワークの責任者を立てていますか？」という質問が生成される。

【０３６９】

このような質問は、上記実施の形態２で述べた「業種によって質問を変更する」手法で生成すればよい。たとえば、業種が金融業である場合には、上記「金融機関等コンピュータシステムの安全対策基準」に則した質問が生成され、インタビューに用いられるのである。このような質問を生成するエキスパートシステムは、上記「金融機関等コンピュータシステムの安全対策基準」に関する情報を含む知識ベースを利用することによって構成することができる。

【０３７０】

このような手法でセキュリティポリシーを構築することによって、より緻密なセキュリティポリシーを構築可能である。

【０３７１】

<u>項目の重複</u>

グローバルガイドラインには存在せず、上記特定の業種の勧告や規定にのみ存在する項目は、もちろん上記特定の業種の勧告や規定に基づきセキュリティポリシーが構築される。

【０３７２】

逆に、グローバルガイドラインにのみ存在し、上記特定の業種の勧告や規定には存在しない項目は、上記実施の形態１と同様にグローバルガイドラインに基づきセキュリティポリシーが構築される。

【０３７３】

さらに、グローバルガイドラインにも存在し、かつ、上記特定の業種の勧告や規定にも存在する項目は、上記特定の業種の勧告や規定に基づきセキュリティポリシーを構築することが好ましい。

【０３７４】

実施の形態４（利用者によるグローバルガイドラインの指定）

これまで、グローバルガイドラインや、特定の業種の勧告や規定に基づくセキュリティポリシーの構築を説明した。

【０３７５】

しかし、利用者が、ある特定のグローバルガイドラインに基づいたセキュリティポリシーを構築したいと望む場合も考えられる。たとえば、ある所定の国（たとえば米国）においては、グローバルガイドラインとして特定のグローバルガイドライン（たとえばＣｏｂｉｔ）がデファクトスタンダードとして利用されている場合がある（Ｃｏｂｉｔに関しては後に説明する）。このような状況下では、セキュリティポリシーもこの特定のグローバルガイドライン（たとえばＣｏｂｉｔ）に基づき構築することが望ましい場合も多い。

【０３７６】

そこで、本実施の形態４では、セキュリティポリシーの構築に際して利用するグローバルガイドライン等を、利用者が明示的に指定可能に構成することを提案する。

【０３７７】

本実施の形態４のセキュリティポリシードラフト構築装置３２０の構成ブロック図が図１０に示されている。この図に示すように、利用者が指示するグローバルガイドラインに関する情報は、質問生成手段３２２とドラフト構築手段３２８とに供給される。

【０３７８】

質問生成手段３２２は、実施の形態１と同様に、メンバーの職務内容に基づいて質問（群）を生成する。本実施の形態５においては、質問生成手段３２２は、質問生成の際に、利用者が指示するグローバルガイドラインに則した質問を生成する。なお、利用者は、１個だけでなく複数個のグローバルガイドラインを指示可能である。

【０３７９】

ドラフト構築手段３２８は、利用者が指示したグローバルガイドラインに基づきセキュリティポリシーのドラフトを構築する。

【０３８０】

本実施の形態５のセキュリティポリシーのドラフト構築の動作は、上記図５に示した動作と、以下の点を除きほぼ同様である。

【０３８１】

第１に異なる点は、ステップＳ５－１において、利用者が指示するグローバルガイドラインに則した質問の生成が行われる点である。

【０３８２】

第２に異なる点は、ステップＳ５－４において、利用者が指示するグローバルガイドラインに則したセキュリティポリシーのドラフトの構築が行われる点である。

【０３８３】

このように本実施の形態５によれば、セキュリティポリシーを構築する際に利用するグローバルガイドライン等を選択することができる。そして、利用者が選択したグローバルガイドラインに則して質問が生成され、その答えに基づいてセキュリティポリシーのドラフトが構築される。その結果、利用者が所望するグローバルガイドラインに則したセキュリティポリシーを構築することが可能である。

【０３８４】

たとえば、利用者が後述するＢＳ７７９９を選択した場合には、ＢＳ７７９９に適合するため（又はさせるため）のセキュリティポリシーを構築することが可能である。

【０３８５】

グローバルガイドライン

グローバルガイドラインとして、広く知られているものの例を以下に示す。

【０３８６】

（１）ＢＳ７７９９

ＢＳ７７９９は、１９９５年に、ＢＳＩ（British Standards Institution：英国規格協会）によって制定された。このＢＳ７７９９は、情報セキュリティにおけるベストプラクティス（最適慣行）をまとめた基本的な管理項目（コントロー

ル）を規定する。

【０３８７】

このＢＳ７７９９の規格は、産業界はもとより行政、あるいはＮＧＯ（Non Governmental Organization：非政府組織）、ＮＰＯ（Non Profit Organization：非営利の民間組織）において、またその組織規模を問わず情報資産を保護する必要がある場合、情報セキュリティの範囲を明確にする際の一つの規範・基準として使用されることを目的としている。

【０３８８】

したがって、後述するＩＳＯ／ＩＥＣ１３３３５「ＩＴ セキュリティマネジメントガイドライン（ＧＭＩＴＳ）」や、ＩＳＯ／ＩＥＣ １５４０８「ＩＴセキュリティ評価基準」などと同様の目的を持った規格である。このＢＳ７７９９がこれら他のグローバルガイドラインと異なる特徴的な点は、次の２点である。

【０３８９】

第一に、他の規格がＩＴを対象としてセキュリティ技術の詳細まで規定しているのに対して、ＢＳ７７９９はマネジメントシステムに対する普遍的、包括的なガイド、基準を示していることである。第二に、電子媒体に限定せず紙媒体など様々な情報資産をセキュリティの対象としていることである。

【０３９０】

近年、このＢＳ７７９９は国際的に非常に注目されている。この理由は、情報セキュリティの詳細な個別コントロールはもちろん重要であるが、ＩＳＯ９０００等システム規格の要求事項にみられるような、（リスク分析に基づき）マネジメントプランを立案し，必要な資源配分及び運用を監視し、客観的に見直すという仕組みが、情報セキュリティマネジメントにも有効であるとの認識が広まったことによるものと言われている。

【０３９１】

ＢＳ７７９９は、第１部：情報セキュリティ管理実施基準及び、第２部：情報セキュリティシステム仕様の２つの部で構成されている。第１部ではベストプラクティスを示し、マネジメントへのアドバイスを与えるガイドラインが示されて

いる。また、第２部は、マネジメントの枠組みを開発すること及び「システム監査」の基準が示されている。この第１部（ＢＳ７７９９－１）が、ＩＳＯ１７７９９としてＩＳＯ化される。

【０３９２】

（２）ＧＡＳＳＰ

ＧＡＳＳＰ（Generally Accepted System Security Principles）は、Ｇｏｏｄ　Ｐｒａｃｔｉｃｅの促進と、リスクの軽減と、リスクの影響の軽減と、を目的とする。ＧＡＳＳＰは、ＯＥＣＤの情報セキュリティ方針を使用して、階層モデル化し、方針を詳細にわたって展開している。

【０３９３】

最上位の基本となる方針は、Pervasive Principlesと呼ばれ、セキュリティの目標概念を掲示している。

【０３９４】

次の階層の方針は、Broad Function Principlesと呼ばれ、Pervasive Principlesの具体的な実行について既述している。

【０３９５】

さらに下の階層の方針は、Detailed Principlesと呼ばれ、環境に応じた詳細なセキュリティガイドラインが記述されている。

【０３９６】

これらの方針は、管理や製品関連のガイドラインだけでなく、個人や組織のプライバシーの管理についても記述している。

【０３９７】

（３）ＧＭＩＴＳ

ＧＭＩＴＳ（The Guidelines for the management of IT Security）は、ＩＳＯ（International Organization for Standardization）によって作成されている。このＧＭＩＴＳは、情報技術のセキュリティに関連した運用管理、計画を対象とした標準を設定することを目的としている。

【０３９８】

ＧＭＩＴＳは、５部から構成されている。

【０３９９】

Part1：Concepts and models for IT Security

このPart1では、情報セキュリティの概要を記述している。

【０４００】

Part2：Managing and Planning IT Security

このPart2では、セキュリティライフサイクルと同様の作業について記述している。

【０４０１】

Part3：Techniques for the managiment of IT Security

このPart3では、Part2に関し、その詳細を記述している。

【０４０２】

part 4：Selection of Safeguards

このpart4では、セキュリティ要件に従ってどのような対応策を選択するのかについて記述している。

【０４０３】

part 5： Management Guidance on Network Security

このpart5は、現在、ドラフト版である。

【０４０４】

ネットワークセキュリティ上の管理に関する作業について記述する。

【０４０５】

（４）ＩＳＯ／ＩＥＣ１５４０８

ＩＳＯ／ＩＥＣ１５４０８は、情報技術を用いた製品やシステムが備えるべきセキュリティ機能に関する要件（機能要件）や、設計から製品化に至る過程でセキュリティ機能が確実に実現されていることの確認を求める要件（保証要件）が集大成された「要件集」である。

【０４０６】

（５）Ｃｏｂｉｔ

Ｃｏｂｉｔ（Control Objectoives for information and related Technology）は、複数の分野にまたがるプロセスのフレームワークに適するセキュリティの

規範（good practice）を示し、管理可能な論理的ストラクチャーを提示する。このgood practiceは、多くの専門家によって得られた同意をもとに作成されている。そして、このＣｏｂｉｔは、業務上のリスクや制御の必要性と技術的問題との間にあるギャップの解消に役立つように設計されているグローバルガイドラインである。

【０４０７】

（６）ＥＵ指令

ここで言うＥＵ指令は、正式には「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」である。このＥＵ指令は、個人データの処理の合法性に関する一般規則が規定されており、データの質に関する原則や、データ処理の適法性の根拠に関する原則や、データの対象者に与えられる情報、データの対象者のデータに対するアクセス権等が、規定されている。

【０４０８】

実施の形態５（強度の指定）

これまでの実施の形態では、セキュリティポリシーの強度の調整は、図１のステップＳ１－４において人為的に行われているのみである。

【０４０９】

しかし、所望のセキュリティポリシーの強度があらかじめ判明している場合には、ステップＳ１－２におけるドラフトの構築段階からその所望の強度を反映させる方が望ましい。

【０４１０】

また、図１のステップＳ１－４においては、各ルールの強度を人為的に調整していた。しかし、強度の指標を定義し、利用者がその指標を用いてセキュリティポリシーの強度を指定し、指定した強度に基づき自動的に各ルールの強度の調整ができれば便利である。

【０４１１】

本実施の形態５において特徴的なことは、図１のステップＳ１－２やステップＳ１－４においてセキュリティポリシーの強度を利用者が客観的に指定可能に構

成していることである。

【０４１２】

このようなことを実現するために、本実施の形態６では、セキュリティポリシーの強度を表す指標を以下のように５種定義している。以下の並びは、強度の強い順である。すなわち、最も強度が強いのが「最高レベル」であり、最も弱いのが「教育機関レベル」である。

【０４１３】

（１）最高レベル：政府や軍事組織で必要と考えられるセキュリティ強度を表す。

【０４１４】

（２）金融レベル：金融機関に必要と考えられるセキュリティ強度を表す。

（３）国際レベル：国際的な企業に必要と考えられるセキュリティ強度を表す。

（４）一般レベル：国内企業に必要と考えられるセキュリティ強度を表す。

（５）教育機関レベル：教育機関に必要と考えられるセキュリティ強度を表す。

【０４１５】

ここでは５段階の例を示したが、もちろん強、中、弱の３段階としてもよい。

【０４１６】

５－Ａ　強度を指定したセキュリティポリシーの構築

ステップＳ１－２（図１）におけるセキュリティポリシーの強度指標の利用について説明する。利用者は、ステップＳ１－２（図１）におけるセキュリティポリシーのドラフトを構築する際に、所望の強度を上記５種から選択してドラフト構築装置２０に指示する。

【０４１７】

この指標に基づき、利用者が所望する強度の規定をグローバルガイドラインから取り出すことによって、利用者の望む強度のセキュリティポリシーのドラフトを構築することが可能である。グローバルガイドラインの中には、セキュリティポリシーの強度を表す指標が含まれているものも多いので、このようなことが可

能である。

【０４１８】

取り出しの動作は、知識ベースの中に各グローバルガイドラインの強度に関する知識を組み込んでおき、この知識ベースを利用して利用者が指示した指標に基づき適切な規定をグローバルガイドラインから取り出すことによって実行される。各グローバルガイドラインの強度に関する知識とは、たとえば、上記５種の強度指標と、この強度指標に対応する規定と、を関連づけた知識である。このような知識を用いることによって、与えられた強度の指標に対応する規定をグローバルガイドライン中から選び出すことが可能である。

【０４１９】

本実施の形態５のセキュリティポリシードラフト構築装置４２０の構成ブロック図が図１２に示されている。この図に示すように、セキュリティポリシードラフト構築装置４２０においては、利用者が指示する強度の指標がドラフト構築手段４２８に与えられる。

【０４２０】

ドラフト構築手段４２８は、利用者が指示した強度指標に基づきセキュリティポリシーのドラフトを構築する。この構築動作は、上述したように、指示された強度指標に基づき、指示された強度指標に合致する方針に関する知識を知識ベースの中に組み入れておき、この知識ベースに基づいて、強度指標に合致した方針をグローバルガイドラインから取り出してくることによって実行される。

【０４２１】

この動作は、要するにある強度指標に対してどのような方針を設定するかに関してあらかじめルールを（知識ベースの中で）取り決めておこうとするものである。

【０４２２】

また、本実施の形態５におけるセキュリティポリシーの構築動作は、以下の点を除き、基本的に図５のフローチャートとほぼ同様である。

【０４２３】

第１に異なる点は、ステップＳ５－１において、質問生成手段４２２が利用者

が指示した強度に基づき、質問を生成する点である。「強度」は、他のパラメータ（業種等）に比べれば質問に対する影響は少ないが、一般的に強度を強くすれば、より細かい事項に関する質問も生成される。また、一般的に強度を弱くすれば、細かい事項に関する質問が新たに生成される。

【０４２４】

たとえば、一度セキュリティポリシーを構築した後で、セキュリティポリシーの強度をより強く設定し直すことが考えられる。この場合、利用者が指示するより強い強度指標は、質問生成手段４２２にも供給されているので、質問生成手段４２２は、より細かい事項に関する質問を生成する。その結果、団体のメンバー（被質問者）に対する質問をもう一度実施する必要性が一部に生じる場合もある。

【０４２５】

一方、セキュリティポリシーの強度をより弱く設定し直した場合には、一般的には、新たな質問が生成される可能性はない。したがって、この場合は、質問をもう一度実施することなく、すぐに新たなセキュリティポリシーの構築を行うことが可能である。

【０４２６】

次に、第２に異なる点は、ステップＳ５－４において、利用者が指示した強度指標がドラフト構築手段４２８にも供給され、ドラフト構築手段４２８が、その強度指標に基づいてセキュリティポリシーのドラフトを構築する点である。

【０４２７】

この２点以外の動作は図５のフローチャートとほぼ同様である。

【０４２８】

５－Ｂ　強度を指定したセキュリティポリシーの調整

本実施の形態５では、ステップＳ１－４（図１）におけるセキュリティポリシーの調整も自動的に実行される。図１２には、そのようなセキュリティポリシーの調整を実行するセキュリティポリシー強度調整装置５００の構成ブロック図が示されている。この図に示すように、セキュリティポリシー強度調整装置５００は、強度検査手段５０２と、強度調整手段５０４と、記憶手段５０６と、合成手

段５０８と、を備えている。

【０４２９】

強度検査手段５０２には、ステップＳ１－３（図１）までの動作で構築されたセキュリティポリシーのドラフトが供給される。この強度検査手段５０２は、利用者が指示する強度の指標に基づき、セキュリティポリシーのドラフト内の各ルールが、利用者が指示する強度に合致しているか否か検査する。検査の結果、各ルールが合致していればそのルールはそのまま出力される。一方、合致していない場合はそのルールは強度調整手段５０４に供給される。強度調整手段５０４は、供給されてきたルールを、利用者が指示する強度指標に基づき、書き換えて出力する。合成手段５０８は、強度指標に合致していたルールと、強度指標に合致するように書き換えられたルールと、を合成し、外部に出力する。記憶手段５０６には、グローバルガイドラインと、グローバルガイドライン中の各ルールと強度指標との対応付けに関する情報と、が記憶されている。

【０４３０】

セキュリティポリシー強度調整装置５００の動作を表すフローチャートが図１３に示されている。

【０４３１】

まず、ステップＳ１３－１において、セキュリティポリシーのドラフトが強度検査手段５０２に供給される。

【０４３２】

ステップＳ１３－２においては、強度検査手段５０２は、供給されたセキュリティポリシーのドラフト中の各ルールが、利用者が指示する強度の指標に合致するか否かを検査する。そして、合致している場合には、後述するステップＳ１３－３に移行する。一方、合致していない場合には、ステップＳ１３－４に移行する。

【０４３３】

ステップＳ１３－４においては、ルールを、利用者が指示する強度の指標に合致するように変更する。この変更は、記憶手段５０６内部のグローバルガイドライン中の各ルールと強度指標との対応付けに関する情報を利用して、強度調整手

段５０４が実行する。この情報は、グローバルガイドライン中の各ルールが対応する強度指標に関する情報であるため、この情報を利用すれば利用者が指示した強度指標に合致したルールを知ることが可能である。そしてこのようにして知ったルールを、同じく記憶手段５０６内部のグローバルガイドラインから取り出し、強度指標と合致しないルールを、この取り出した合致するルールと置き換えるのである。

【０４３４】

ステップＳ１３－３においては、強度指標に合致していたルールと、変更したルールと、が合成されて出力される。この合成出力動作は、合成手段５０８によって実行される。

【０４３５】

このようにして、セキュリティポリシーのドラフト内の各ルールを、利用者が指示する強度の指標に合致させることができる。

【０４３６】

なお、本実施の形態５における強度検査手段５０２、強度調整手段５０４、合成手段５０８は、コンピュータ上で動作するソフトウェアで構成することが好ましい。また、記憶手段５０６は、ハードディスク、ＣＤ－ＲＯＭ、ＤＶＤ等の種々の記憶媒体で構成することが望ましい。

【０４３７】

ルールと強度指標の関係

ステップＳ１３－２におけるルールの強度と、利用者が指示する強度指標で表される強度とが合致しない場合についてより詳細に説明する。

【０４３８】

ルールが強度指標で示される強度より弱い強度のルールである場合には、そのルールは強度指標に合致していないと判断され、より強い強度のルールと置き換えられる。

【０４３９】

たとえば、ルールが教育機関レベルであり、利用者が指示した強度が金融レベルである場合には、そのルールは金融機関レベルのルールに置き換えられるので

ある。また、たとえば、パスワードの有効期間が１２０日から３０日に短縮され、より厳しい（強い）レベルのルールに置き換えられるのである。

【０４４０】

そして、ルールが強度指標で示される強度より強い強度のルールである場合には、そのルールは強度指標に合致していないと判断され、より弱い強度のルールと置き換えられる。

【０４４１】

たとえば、ルールが最高レベルであり、利用者が指示した強度が一般レベルである場合には、そのルールは一般レベルのルールに置き換えられるのである。また、たとえば、パスワードの保存期間が、最高レベルでは１週間であるが、それでは厳しすぎる場合、利用者は一般レベルを指定する。すると、たとえばパスワードの有効期間が１００日に延長され、より緩い（弱い）レベルのルールに置き換えられるのである。

【０４４２】

実施の形態６（構築範囲の選択）

これまで述べた例においては、セキュリティポリシーはその団体の全体に対して作成されている。しかしながら、その団体の一部のシステムに対してのみセキュリティポリシーを構築したいという要望も多いと考えられる。

【０４４３】

そこで、利用者がセキュリティポリシーを構築する範囲を指定し、この範囲に基づいてセキュリティポリシーを構築する装置・方法を採用すれば、利用者がセキュリティポリシーを構築したいと考える部分に対してのみセキュリティポリシーを構築することができ便利である。

【０４４４】

図１４には、このようなセキュリティポリシードラフト構築装置５２０の構成を表す構成ブロック図が示されている。この図に示すセキュリティポリシードラフト構築装置５２０の構成は、図１０や図１１で説明したセキュリティポリシー構築装置３２０や４２０と同様である。

【０４４５】

異なる点は、以下の２点である。

【０４４６】

・ドラフト構築手段５２８に利用者が指示するセキュリティポリシーの構築範囲が供給されている点。

【０４４７】

・質問生成手段５２２に利用者が指示するセキュリティポリシーの構築範囲が供給されている点。

【０４４８】

このような構成によって、ドラフト構築手段５２８は、利用者が指示する範囲に関するセキュリティポリシーを構築するので、利用者は必要な範囲のセキュリティポリシーを効率的に得ることが可能となる。

【０４４９】

また、質問生成手段５２２も利用者が指示する範囲に関する質問のみを生成するので、無駄な質問がなくなり、効率的な質問を行うことができる。ただし、質問生成手段５２２には、必ずしも利用者が指示する範囲が供給されなくてもよい。質問が多くてもセキュリティポリシーの構築には影響がないからである。また、利用者が指示した範囲と関係ない質問の場合にはインタビュー時に、質問者が質問をスキップすることもできる。したがって、利用者が指示した範囲が質問生成手段に５２２に供給されていることは必須の要件というわけではない。

【０４５０】

さて、利用者は、セキュリティポリシーの構築範囲を種々の手法で指示することができる。

【０４５１】

（１）まず、利用者はセキュリティポリシーの構築範囲をプロダクト（製品）のレベルで指示することができる。たとえば、利用者は「ＶＰＮ」に関するセキュリティポリシーのみを構築したい場合は、この「ＶＰＮ」を指示することにより、ＶＰＮに関するセキュリティポリシーを構築させることができる。また、ＷＥＢ、Ｅメール、ファイアーウォール、等の具体的なハードウェアやソフトウェア、もしくは機能を指示することによって、利用者はその具体的なハードウェア

やソフトウェアに関するセキュリティポリシーの構築を指示することができる。

【０４５２】

（２）次に、利用者は、使用目的によってセキュリティポリシーの構築範囲を指示することができる。たとえば、利用者は「外部委託」に関するセキュリティポリシーのみを構築したい場合は、この「外部委託」を指示することにより、外部委託を実行する部分に関してセキュリティポリシーを構築させることができる。また、電子商取引（Ｅコマース）、データセンター、等の具体的な使用目的、もしくは用途を指示することによって、利用者はその使用目的や用途に関する範囲のセキュリティポリシーの構築を指示することができる。

【０４５３】

（３）さらに、利用者は、団体の組織としての観点からセキュリティポリシーの構築範囲を指示することができる。たとえば、利用者は「本社」に関するセキュリティポリシーのみを構築したい場合は、この「本社」を指示することにより、本社に関するセキュリティポリシーを構築させることができる。また、支店を指示することによって、支店のセキュリティポリシーを構築させることができる。さらに、利用者は、ネットワークや、ホスト等を指示することによって、ネットワークに関するセキュリティポリシー、ホストに関するセキュリティポリシーをそれぞれ構築させることができる。

【０４５４】

本実施の形態７のセキュリティポリシー構築の動作は、上記図５に示した動作とほぼ同様である。異なる点は以下の通りである。

【０４５５】

・第１に、図５におけるステップＳ５－４において、利用者が指示する範囲に基づき、セキュリティポリシーのドラフトの構築が行われる点である。

【０４５６】

・第２に、図５におけるステップＳ５－１において、利用者が指示する範囲に関する質問のみが生成される点である。

【０４５７】

この第２の相違点は、必ずしも必須の要件ではない。既に説明したように、質

問が、利用者が指示した範囲外のものであっても、セキュリティポリシーの構築には直接には支障がないからである。また、質問者が適宜そのような質問をスキップすることも考えられるので、質問自体は、実施の形態１などと同様でもかまわない。

【０４５８】

このセキュリティポリシーのドラフトの構築は、図１４のドラフト構築手段５２８が実行する。このようなことを実現するために、記憶手段５２４中には、グローバルガイドライン中の各ルールが、どの範囲にあるかについての知識ベースが構築されている。すなわち、各ルールが、「本社」の範囲にあるのか、それとも「支店」の範囲にあるのか、等の知識ベースが記憶手段５２４中に格納されている。この知識ベースを参照することによって、ドラフト構築手段５２８は、利用者が指示した範囲に含まれるルールのみを用いてセキュリティポリシー（のドラフト）を構築する。

【０４５９】

このようにして、本実施の形態７によれば、利用者が指示した構築範囲に基づき、その範囲のセキュリティポリシー（のドラフト）の構築を行うことができる。

【０４６０】

なお、本実施の形態６では、実施の形態１と同様に質問生成手段５２２がメンバー（被質問者）の職務内容に応じて質問を生成する例を示したが（図１４）、質問生成手段が職務内容に関わらず一般的な質問をメンバーに対して行う構成としてもよい。

【０４６１】

実施の形態７（プログラム及び記録媒体）

これまで述べた各実施の形態における各手段は、実際には、プログラム及びそのプログラムを実行するプロセッサから構成することが好適である。

【０４６２】

図１５には、コンピュータと各種のプログラムが格納されたハードディスク装置６００を備えたコンピュータ６０２が示されている。

【０４６３】

このハードディスク６００中には、上述した各実施の形態１～７で説明した質問生成手段１２や、回答保管手段１６、ドラフト構築手段１８等の各手段の動作を実行するプログラムが格納されている。コンピュータ６０２のプロセッサがこれらのプログラムを実行することによって、このコンピュータ６０２は、質問生成手段や、回答保管手段、ドラフト構築手段等に相当する動作を実行可能である。

【０４６４】

また、図７における矛盾検査手段３２や、矛盾出力手段４０、整合手段４１、仮想構築手段３４、差異出力手段３８、実システム入力手段３６等の動作を実行するプログラムもハードディスク６００中に格納されている。コンピュータ６０２のプロセッサがこれらのプログラムを実行することによって、このコンピュータ６０２は、矛盾検査手段３２等の動作を実行可能である。

【０４６５】

また、上記実施の形態で説明した記憶手段１４等はハードディスク６００内に設けるのが好適である。

【０４６６】

このようなコンピュータ６０２の操作者は、上記各種プログラムを起動し、質問を生成し、団体のメンバーから得た回答をキーボード６０４から入力すること等を実行することができる。もちろん、回答の入力は、マウス等の入力デバイスを用いて実行してもかまわない。

【０４６７】

なお、図１５においては、いわゆるスタンドアローンでプログラムがコンピュータ６０２上で動作する例を示したが、ネットワークを介してプログラムを供給する形態を採用してもよい。

【０４６８】

たとえばサーバに上記各種プログラムが格納されており、そのプログラムを実行する必要がある度に、クライアントコンピュータがサーバ内のプログラムを実行したり、ダウンロードして使用する形態を採用することも好ましい。

【０４６９】

セキュリティポリシーのドラフトについて

これまで述べた各実施の形態１～８においては、セキュリティポリシーのドラフトの構築に関して主に述べたが、ドラフトではないセキュリティポリシーの構築に使用できることは言うまでもない。すなわちセキュリティポリシードラフト構築装置は、セキュリティポリシーの構築装置でもあり、セキュリティポリシーのドラフト構築の方法は、セキュリティポリシー構築方法でもある。また、ドラフト構築手段は、セキュリティポリシーの構築手段でもある。

【０４７０】

【発明の効果】

以上述べたように、本発明によれば、団体のメンバーに質問をすることによって、その回答に基づき、セキュリティポリシーを構築している。したがって、セキュリティポリシーを容易に構築することができる。

【０４７１】

さらに、本発明によれば、段階的にセキュリティポリシーの構築を行っているため、団体の要望（予算など）に応じた柔軟な構築方法を実行することが可能である。

【０４７２】

また、本発明によれば、団体の情報セキュリティの状況を診断するので、団体は情報セキュリティの重要性を知ることができる。

【０４７３】

また、本発明によれば、セキュリティ対策を優先度と共に知ることができるため、将来の情報セキュリティ対策の計画を立案しやすくなる。さらに、この計画に基づき、団体の予算の検討を行うことが可能となる。

【０４７４】

また、本発明によれば、利用者が、セキュリティポリシーの構築に際して使用するグローバルガイドラインを指示可能である。

【０４７５】

また、本発明によれば、グローバルガイドライン以外の特定の業種向けの規定

・勧告を使用してセキュリティポリシーを構築しているので、各業種により合致した緻密なセキュリティポリシーを構築可能である。

【０４７６】

また、本発明によれば強度指標を用いて利用者がセキュリティポリシーの強度を指示可能である。また、本発明によれば、強度指標を用いてセキュリティポリシーの強度を調整することができる。

【０４７７】

また、本発明によれば、利用者がセキュリティポリシーの構築範囲を明示的に指示可能である。その結果、団体の部分的なセキュリティポリシーの構築を実行することができる。

【図面の簡単な説明】

【図１】

本発明の好適な実施の形態１のビジネスモデルの原理を表すフローチャートが示されている。

【図２】

評価装置の構成ブロック図である。

【図３】

評価書の作成作業の動作を表すフローチャートである。

【図４】

セキュリティポリシードラフト構築装置の構成ブロック図である。

【図５】

セキュリティポリシードラフト構築装置を用いてセキュリティポリシーのドラフトを構築する動作を表すフローチャートである。

【図６】

職務内容を表すタイプの一覧表を示す図である。

【図７】

分析装置の構成ブロック図である。

【図８】

実施の形態２のセキュリティポリシードラフト構築装置の構成ブロック図であ

る。

【図９】

実施の形態３のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図１０】

実施の形態４のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図１１】

実施の形態５のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図１２】

実施の形態５のセキュリティポリシー強度調整装置の構成ブロック図である。

【図１３】

実施の形態５のセキュリティポリシー強度調整装置の動作を表すフローチャートである。

【図１４】

実施の形態６のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図１５】

実施の形態７におけるコンピュータ及びその内部のハードディスクを示す説明図である。

【符号の説明】

１０　評価装置

１２　質問出力手段

１４　記憶手段

１６　回答保管手段

１８　セキュリティ完成度作成手段

２０　セキュリティポリシードラフト構築装置

２２　質問生成手段

２４　記憶手段

２６　回答保管手段

２８　ドラフト構築手段

３０　分析装置

３２　矛盾検査手段

３４　仮想構築手段

３６　実システム入力手段

３８　差異出力手段

４０　矛盾出力手段

４１　整合手段

１２０　セキュリティポリシードラフト構築装置

１２２　質問生成手段

１２４　記憶手段

１２６　回答保管手段

２２０　セキュリティポリシードラフト構築装置

２２２　質問生成手段

２２４　記憶手段

２２６　回答保管手段

２２８　ドラフト構築手段

３２０　セキュリティポリシードラフト構築装置

３２２　質問生成手段

３２４　記憶手段

３２６　回答保管手段

３２８　ドラフト構築手段

４２０　セキュリティポリシードラフト構築装置

４２２　質問生成手段

４２４　記憶手段

４２６　回答保管手段

４２８　ドラフト構築手段

５００　セキュリティポリシー強度調整装置

５０２　強度検査手段

５０４　強度調整手段

５０６　記憶手段

５０８　合成手段

５２０　セキュリティポリシードラフト構築装置

５２２　質問生成手段

５２４　記憶手段

５２６　回答保管手段

５２８　ドラフト構築手段

６００　ハードディスク

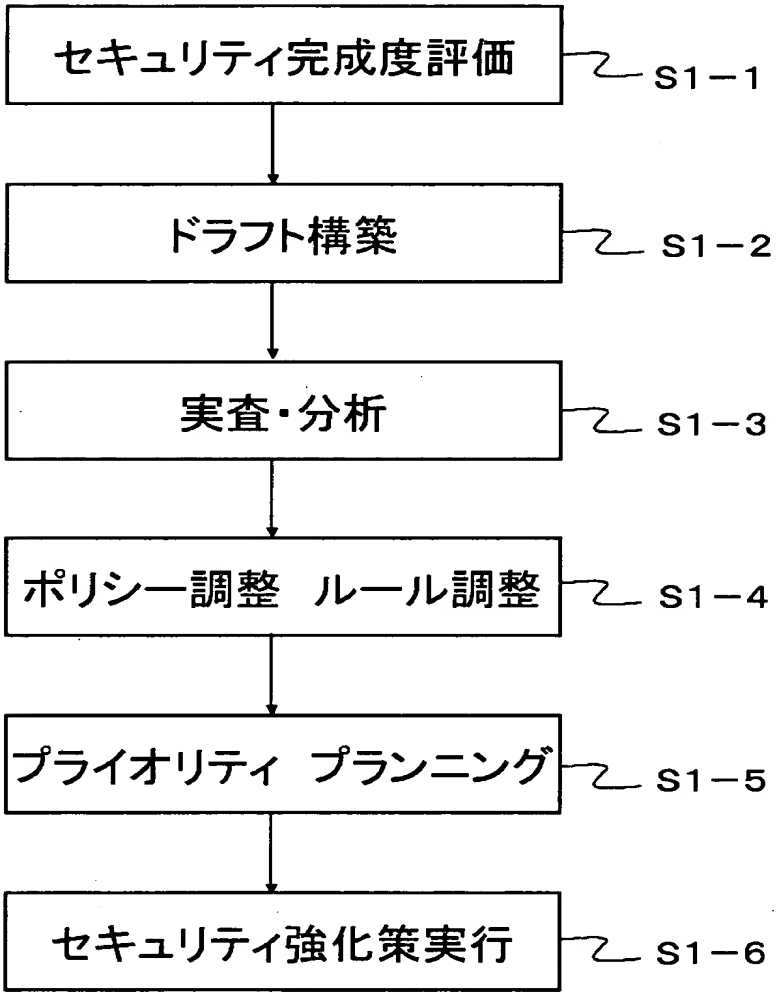
６０２　コンピュータ

６０４　キーボード

【書類名】　図面

【図１】

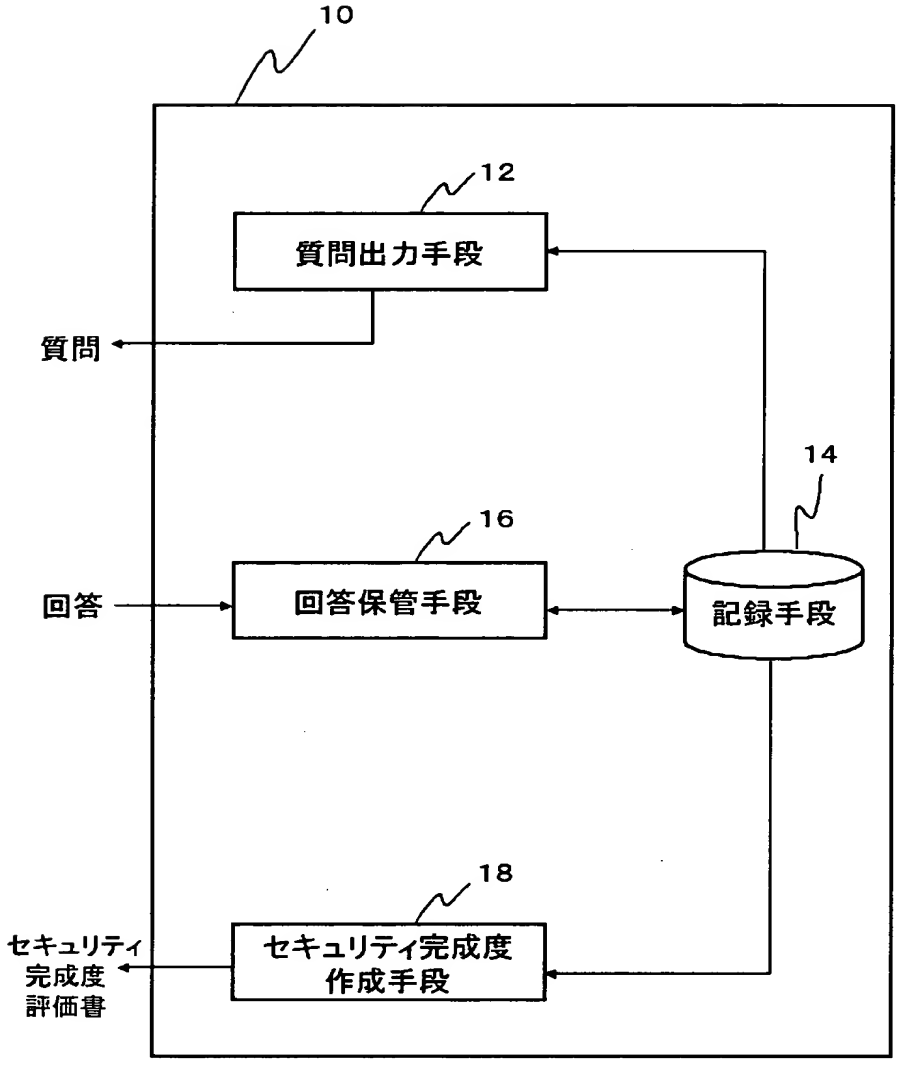
図1　ASG－0002



【図２】

図2

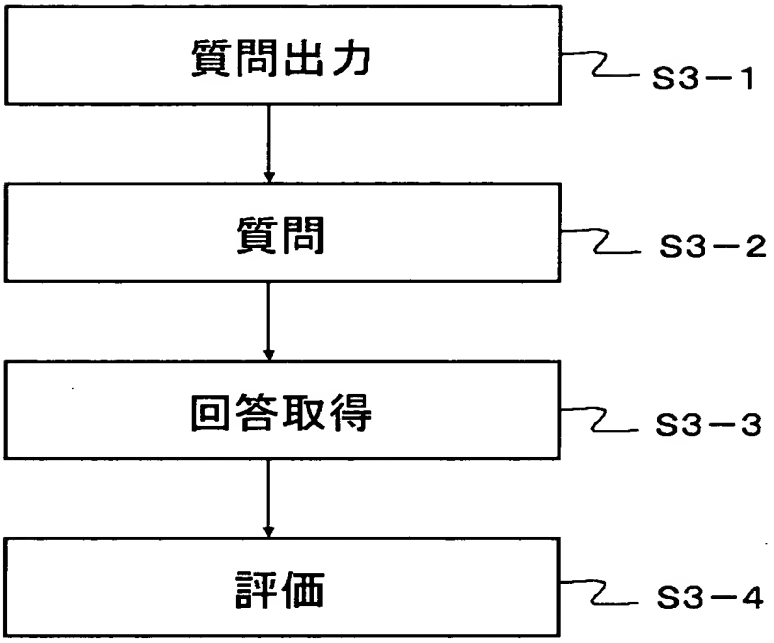
ASG－0002



【図３】

図3

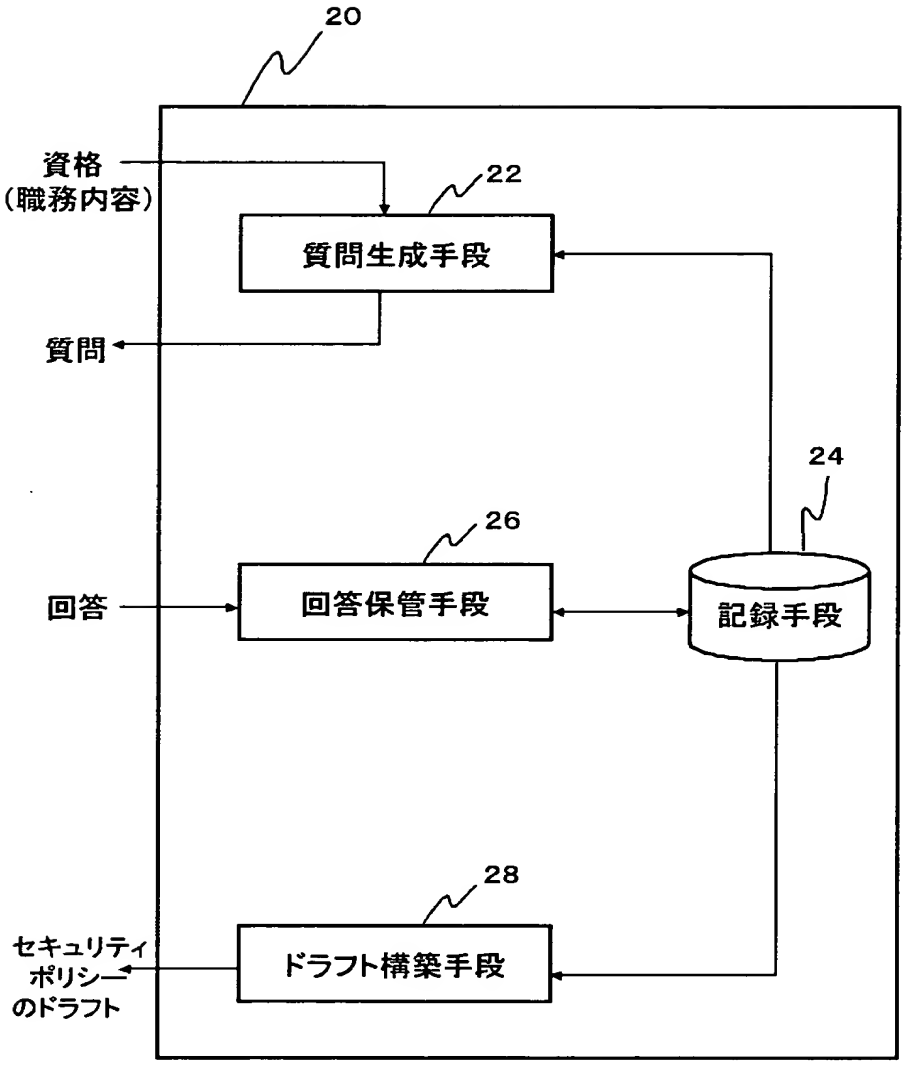
ASG－0002



【図４】

図4

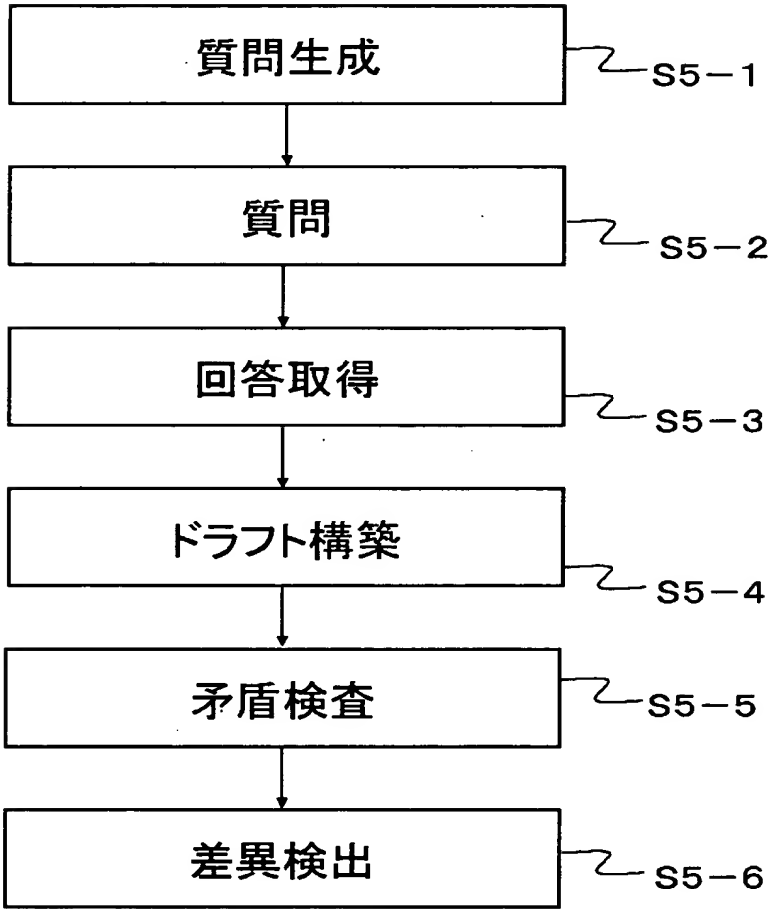
ASG－0002



【図５】

図5

ASG－0002



【図６】

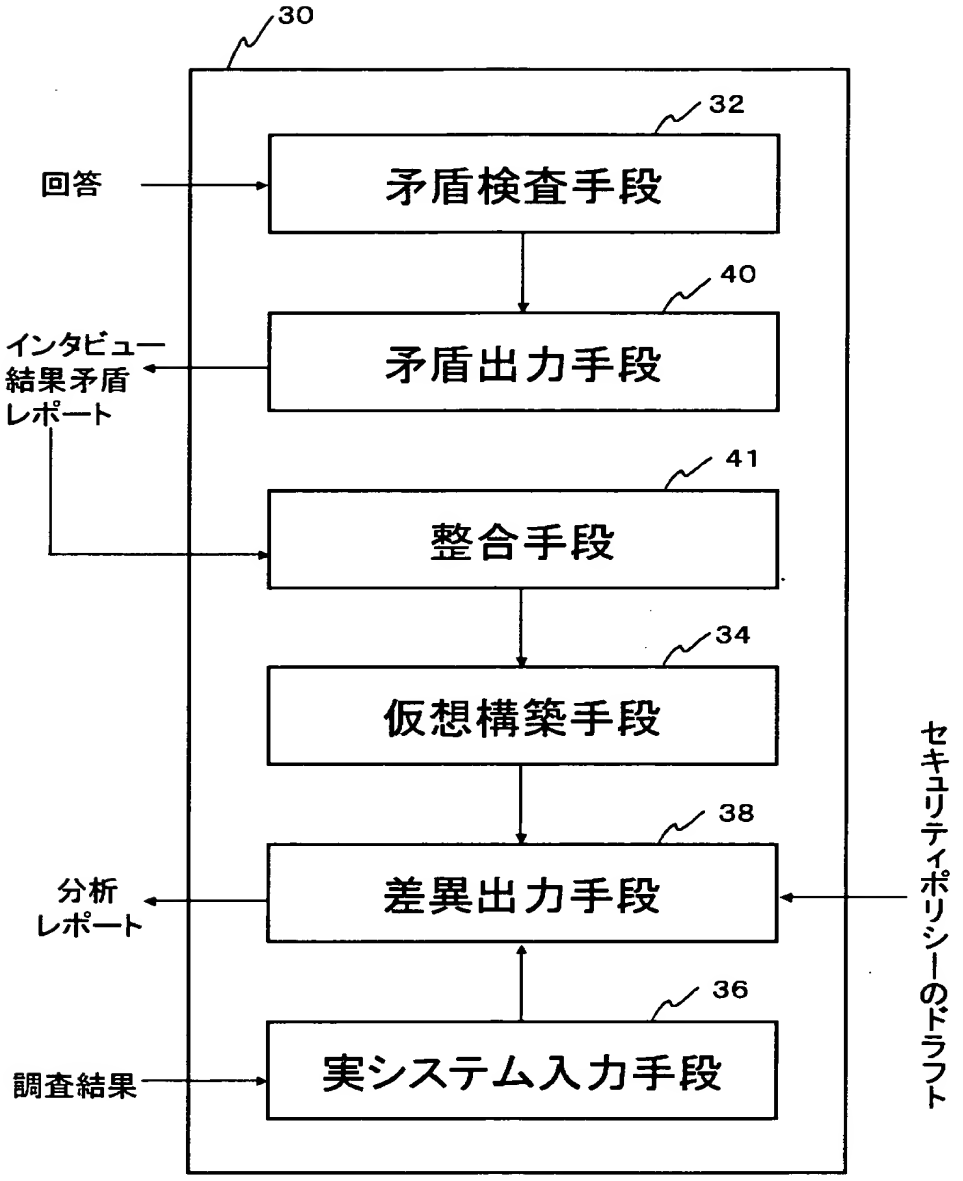
図6　　ASG－0002

タイプ	定義
アプリケーション管理者[APP]	アプリケーション、またはアプリケーションのグループの運用管理者
アプリケーションセキュリティ管理者[ASA]	アプリケーション、またはアプリケーションのグループのローカルセキュリティ運用管理者
内部監査役員[AUD]	内部監査を担当する役員
社長／最高経営責任者[CEO]	社内の業務、運営、またはその他全般に関わる最終決定権を持つ役員、または社長。
情報統括役員[CIO]	情報統括役員。単なるコンピュータ担当者とは違い、企業戦略として情報システムの活用方法を立案、実行する情報資源管理の責任をもつ。情報、通信部門の最高責任者でもある。
災害復旧統轄役員[DDR]	災害復旧を担当する上級役員
ダイヤルイン管理者[DIA]	ネットワークセグメント、または部門のダイヤルイン担当の管理者
情報保護役員[DIP]	情報セキュリティ担当の役員
災害復旧管理者[DRA]	ネットワークセグメント、ホストまたはアプリケーションについての各部のセキュリティ管理者
部門セキュリティ管理者[DSA]	ローカルのネットワークセグメント、ホスト、またはアプリケーションについての各部のセキュリティ管理者
通信担当役員[DTC]	電話回線、広範囲なネットワーク接続を含む電気通信を担当する役員
Facilitator[FAC]	インタビュー実施者
ファイアウォール管理者[FWA]	ファイアウォールのホストシステムの運用管理者
人事[HR]	従業員の採用、教育を担当する部門
ホスト管理者[HST]	ローカルホスト、またはローカルホストのグループ運用管理者
法律担当役員[LEG]	法律顧問
ネットワークセグメント[Net]	ネットワークセグメント、またはネットワークセグメントのグループ運用管理者
ユーザデスクトップ管理者[PCA]	ローカルユーザデスクトップコンピュータを担当する運用管理者

【図７】

図7

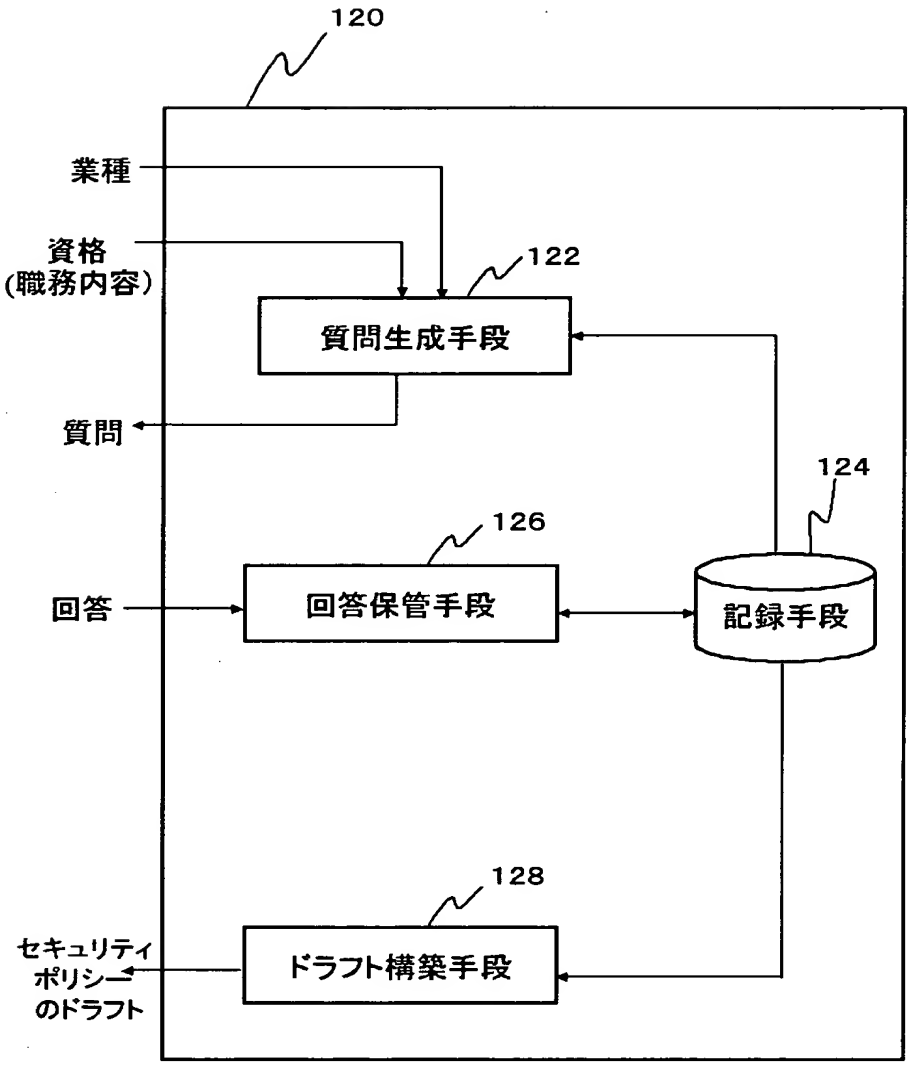
ASG－0002



【図８】

図8

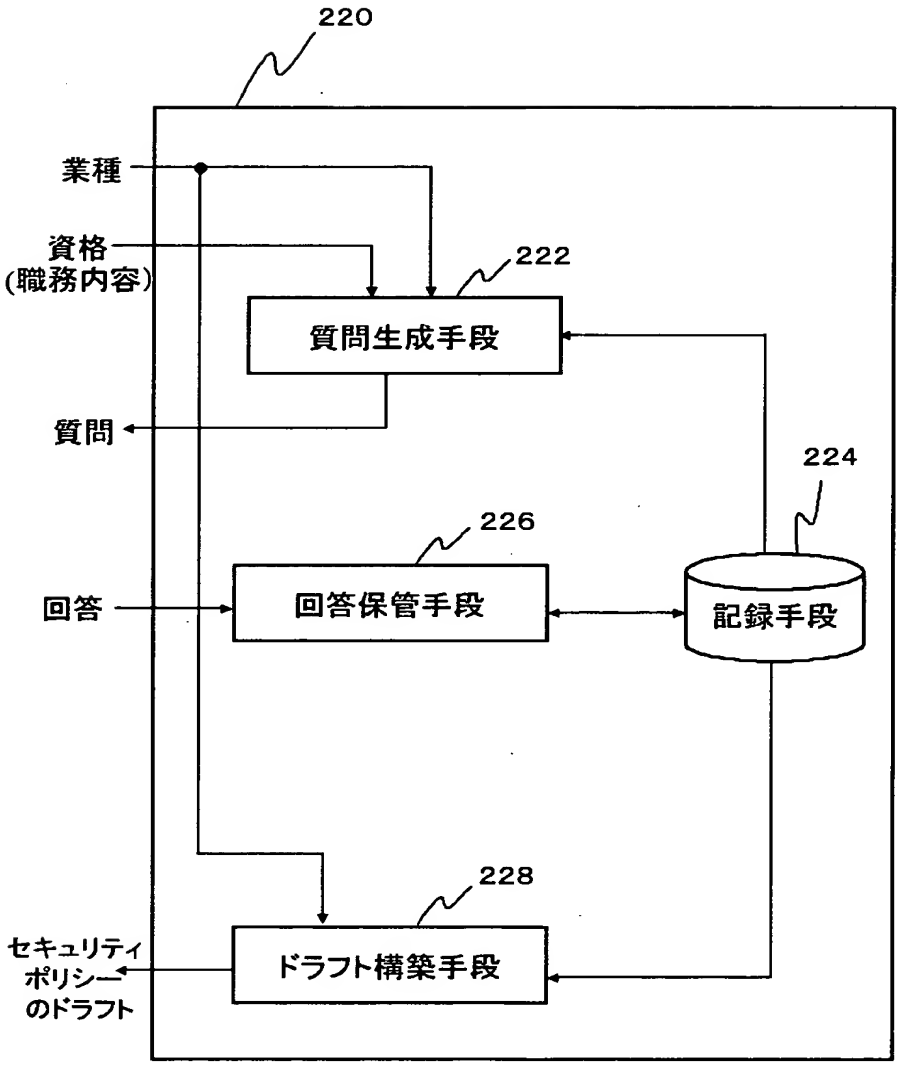
ASG－0002



【図９】

図9

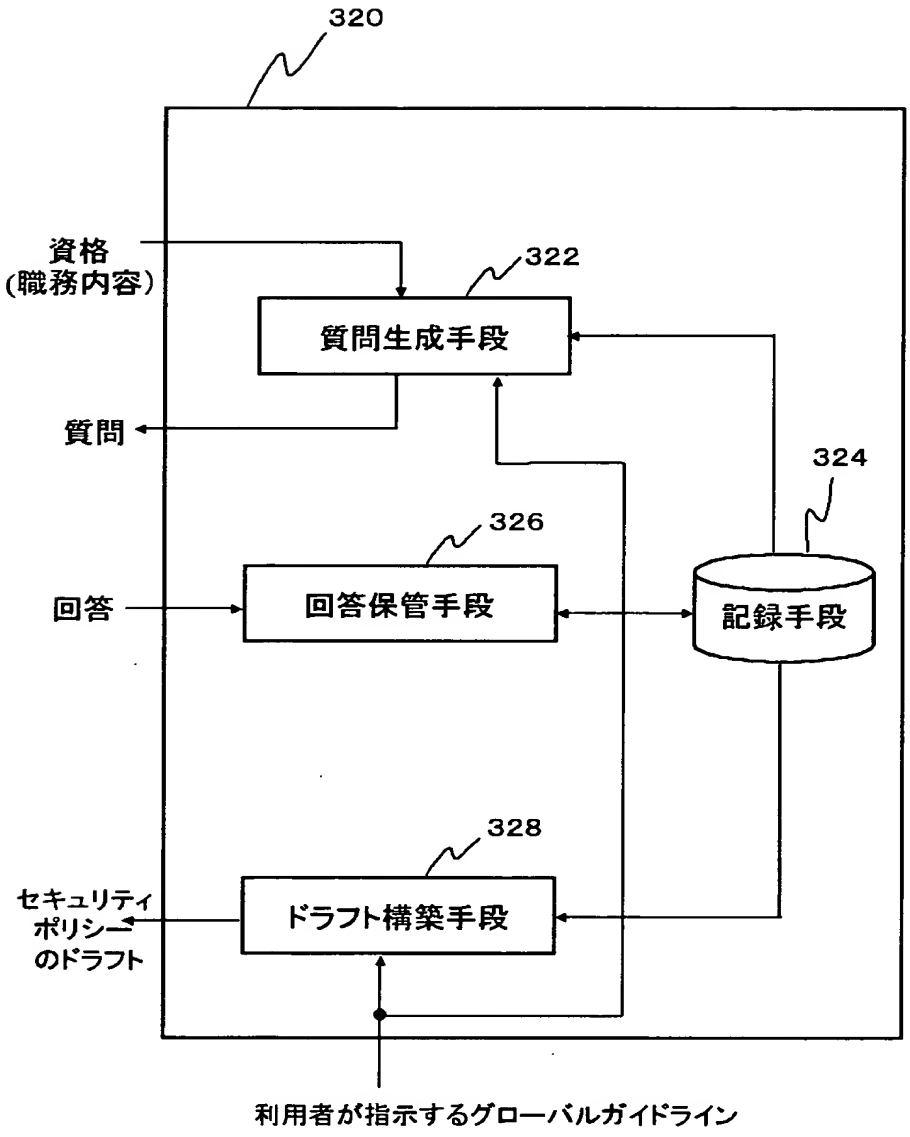
ASG−0002



【図１０】

図10

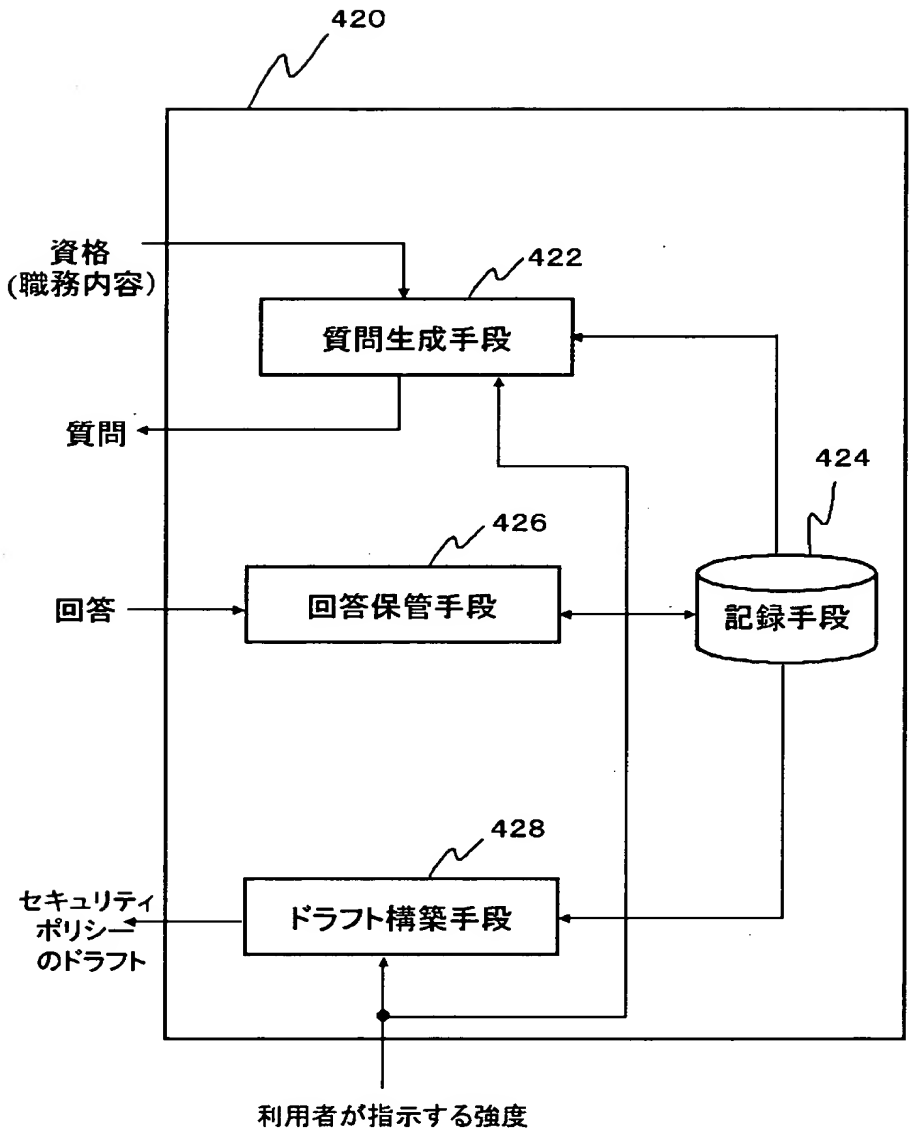
ASG－0002



【図１１】

図11

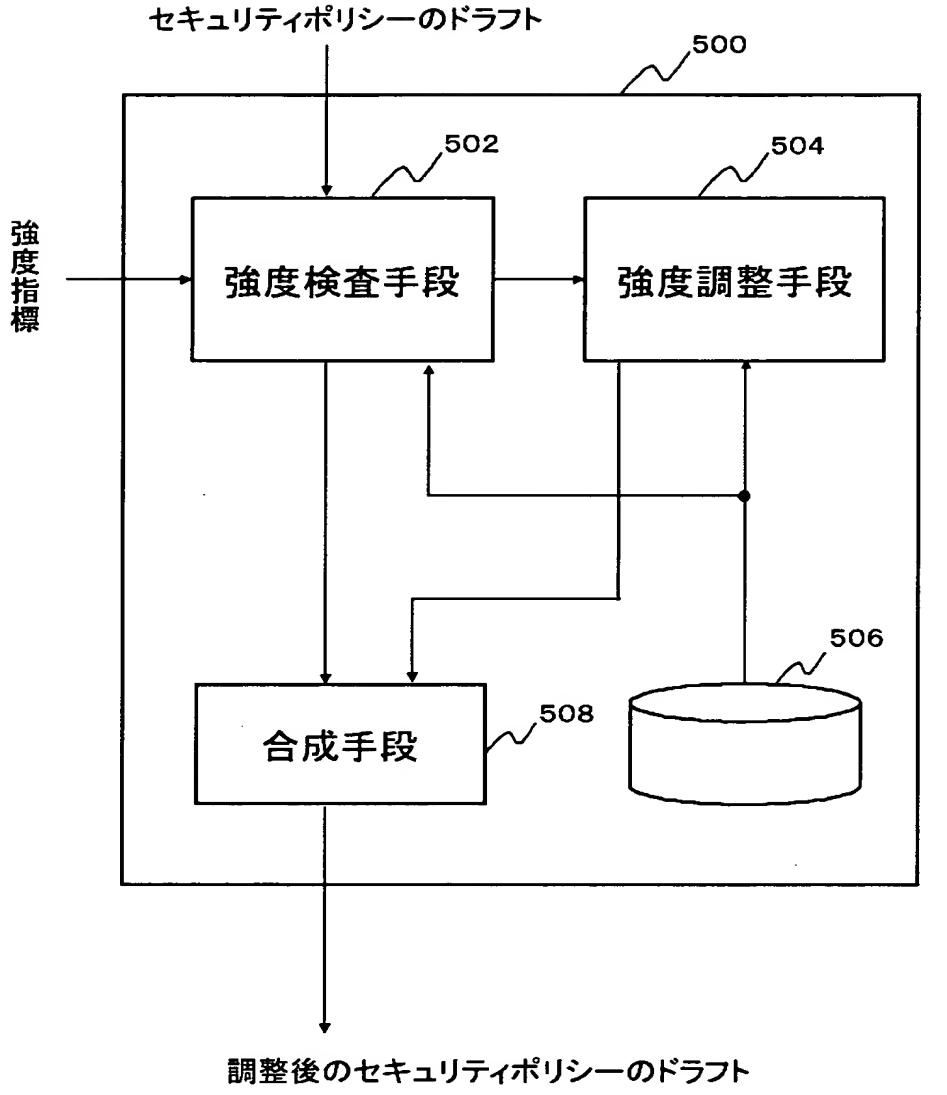
ASG－0002



【図１２】

図12

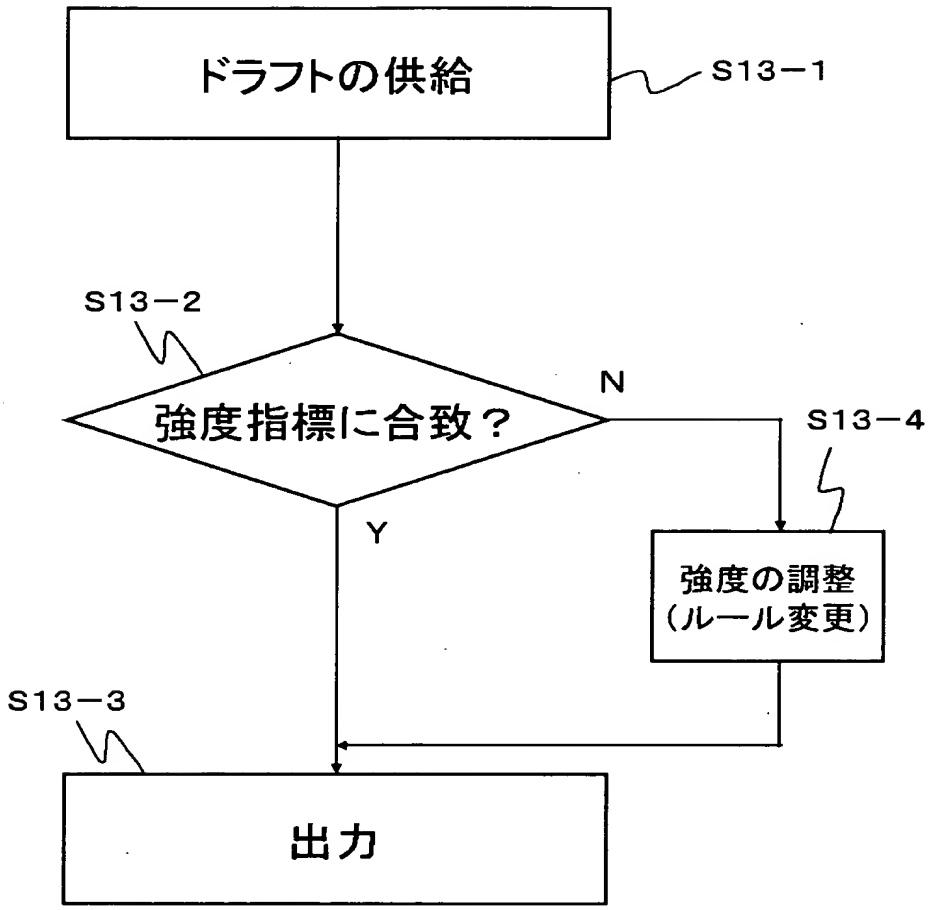
ASG－0002



【図１３】

図13

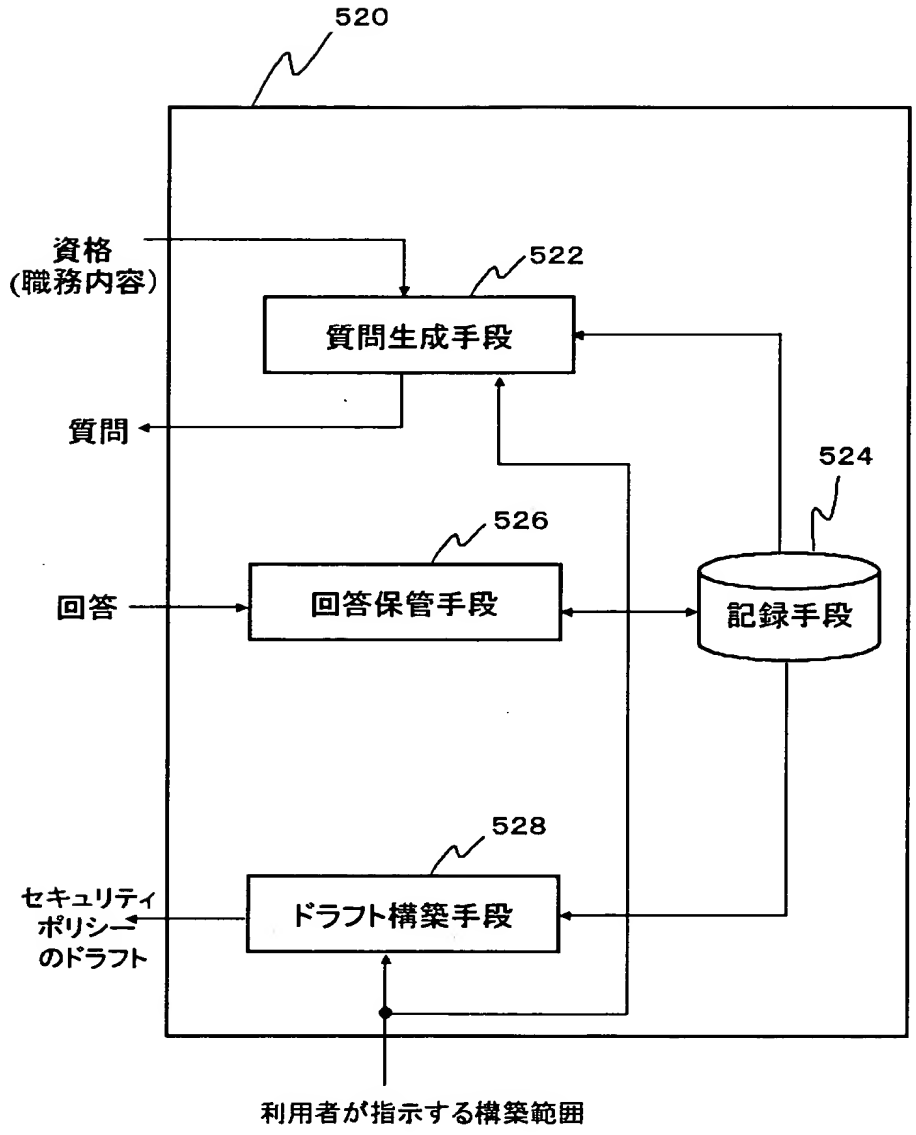
ASG－0002



【図１４】

図14

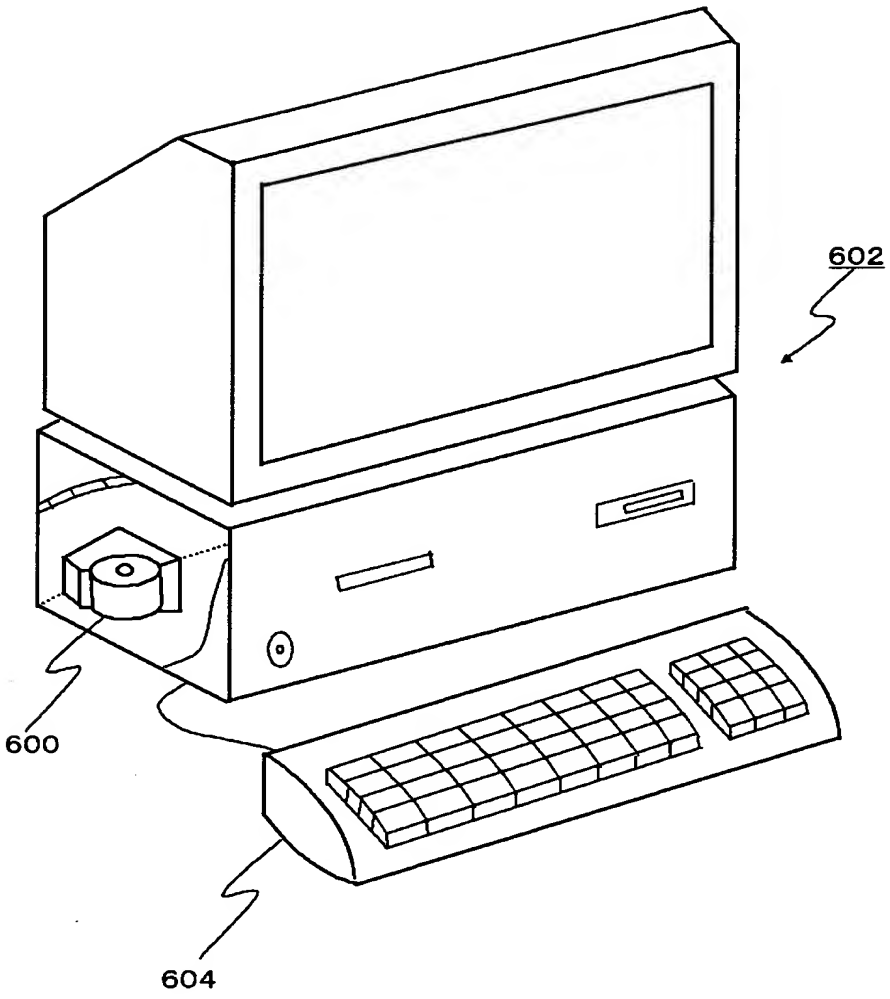
ASG－0002



【図１５】

図15

ASG－0002



【書類名】　要約書

【要約】

【課題】　セキュリティポリシーを効率的に構築する方法及びセキュリティポリシーの構築を支援する装置を提供することである。

【解決手段】　６段階のステップからなるセキュリティ構築手法によれば、最初は簡易にセキュリティポリシーのドラフトを構築し、必要に応じ、団体の実態との再調整を行い、段階的に、セキュリティポリシーを完成していくので、各団体のスケジュールや予算に合わせてセキュリティポリシーを構築することが可能である。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔５００００５６４４８〕

１．変更年月日　　２０００年　２月１０日
［変更理由］　新規登録
住　所　　東京都中央区日本橋小網町１９－７
氏　名　　株式会社アズジェント